



Lightweight ECC Based Multifactor Authentication Protocol (LEMAP) for Device to Device Cellular Network

Rashad Mahmood Saqib

Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
2022

Rashad Mahmood Saqib

Doctor of Philosophy

2022

Lightweight ECC Based Multifactor Authentication Protocol (LEMAP) for
Device to Device Cellular Network

Rashad Mahmood Saqib

A thesis submitted

In fulfillment of the requirement for the degree of Doctor of Philosophy

Computer Science

Faculty of Computer Science and Information Technology
UNIVERSITI MALAYSIA SARAWAK

2022

DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Malaysia Sarawak. Except where due acknowledgements have been made, the work is that of the author alone. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

.....

Signature

Name: Rashad Mahmood Saqib

Matric No.: 15010175

Faculty of Computer Science and Information Technology

Universiti Malaysia Sarawak

Date :

DEDICATION

To the Almighty ALLAH (SWT) and the Holy Prophet Muhammad (P.B.U.H)

&

Also dedicated to my great and very beloved father Mr. Ali Asghar, my beloved mother Haleema Bibi, my brother Shaukat Ali, my sisters, wife and my beloved son Usman Rashad, Umer Shaukat, Zunaira Shaukat, Umaira Shaukat. Special dedication to my best friend Dr. Yasir Javed Kiani for his great support, guidance and mentor Dr. Adnan Shahid Khan who always motivated, guided and encouraged me in achieving this milestone of life.

ACKNOWLEDGEMENT

I owe my gratitude to ALLAH (SWT), the most gracious and the most merciful Whose guidance and protection sustained me throughout my entire life and makes my educational career a reality with enormous success. Special gratitude goes to my supervisor Senior Lecturer Dr. Adnan Shahid Khan for his proper supervision, motivation, fatherly advice, support and encouragement throughout the entire study period at Universiti Malaysia Sarawak. His knowledge and expertise in D2D Security will always remain with me as guidance to follow. Without his guidance, the research and achieving this milestone of life would have been impossible. I would also like to thank my co-supervisors, Associate Professor Dr Nazim Jambli for his sincere advice.

My special and profound gratitude goes to my late father Ali Asghar, mother Haleema Bibi and sisters, niece Zunaira Shaukat and my entire family members and friends for their support and prayers. Immense gratitude and special thanks to my wife and son Usman Rashad for their constant prayers, patience, tolerance and sense of understanding.

I would like to sincerely appreciate the effort and assistance of my beloved friend Dr. Yasir Javed Kiani for his constant support, guidance and sincere advice towards the successful completion of the programme. I would like to say special thanks to my colleagues and friends for their advice, encouragement and prayers. The contributions of authors whose work have being duly cited in this research are hereby acknowledged. I am grateful to all.

My sincere gratitude to the Centre for Graduate Studies, for the advice and support given during my period of study in Universiti Malaysia Sarawak.

Finally, I would like to thank the management of the Universiti Malaysia Sarawak for making it possible for me to complete my study here in Sarawak. Thank you all.

ABSTRACT

Device to Device (D2D) communication is a type of technology where two devices can communicate directly with each other without the need to contact Base Station or any central infrastructure. With emerging of Long Term Evaluation (LTE) and Fifth Generation (5G) technology, D2D has gained a lot of attention for communication between closely located mobile devices for offering high speed, energy efficiency, throughput, less delay, and efficient spectrum usage. D2D has changed recent wireless networks with new trends as D2D can play a vital role in sharing resources by load off the network in local areas by direct communication between devices and useful in natural disasters where BS is destroyed. D2D has revolutionized the direct communication as it is a basis for 5G network. D2D allows miniature devices like cell phone, tablets and radio devices to work as Non-Transparent Relays (NTR) where they can provide services as well as forward traffic, request services by direct communication without the need of Base Station (BS) or central network infrastructure. Multi-hop D2D can be used for peer-to-peer communication or even access to cellular networks. This concept of multihop D2D communication has introduced a number of issues and challenges that were not prevalent in traditional current cellular communication. One of the major issues in D2D is security that is required in D2D communication to transmit information securely over non secure channel. The major challenge when considering security is that current established security techniques cannot be modified as security-requiring devices are miniature with restricted processing and storage or are constrained by power and bandwidth issues. Another issue is that how devices can get secure mutual authentication for secure communication. To tackle these issues, a lightweight multifactor authentication scheme that allows multihop secure communication over open channel is designed called as Lightweight ECC based Multifactor Authentication

Protocol (LEMAP) in multihop D2D communication. Formal analysis of scheme is performed using well known BAN Logic method which is used to check correctness of protocol. The formal analysis of LEMAP proves that it can mitigate replay attack, Man-in-the-Middle (MITM) attack, Rogue device attack, Denial of Service (DoS) attack, timestamp exploitation attack, impersonation attack and masquerading attack. LEMAP also achieves security requirements confidentiality, integrity, privacy, non-repudiation, secure mutual authentication and anonymity. The communication cost and computational overhead of benchmark protocols and the proposed scheme LEMAP are also calculated. The results show that LEMAP is 6%-28% percent stronger than the selected benchmark algorithms such as 2PAKEP, Chaotic based authentication and TwoFactor authentication protocol. Additionally, LEMAP provides additional security by using trust validation, double hashing, and reduced authentication overhead. Discrete logarithm analysis shows that LEMAP is more secure compared to current security algorithms or current security algos are used as attacks against LEMAP. LEMAP is a lightweight and flexible scheme which can be used in 5G as well as multihop D2D communication to provide secure communication environment.

Keywords: D2D security, multihop D2D security, multi factor, light-weight security, ECC

***Protokol Pengesahan Multifaktor Berbasis ECC Ringan (LEMAP) untuk Rangkaian
Selular Peranti ke Peranti***

ABSTRAK

Komunikasi Peranti ke Peranti (PkP) adalah sejenis teknologi di mana dua peranti dapat berkomunikasi secara langsung antara satu sama lain tanpa perlu menghubungi Stesen Pangkalan atau infrastruktur pusat. Dengan munculnya teknologi LTE dan 5G, D2D telah mendapat banyak perhatian untuk komunikasi antara peranti mudah alih yang terletak berdekatan untuk menawarkan kelajuan tinggi, kecekapan tenaga, throughput, penundaan yang lebih sedikit, dan penggunaan spektrum yang efisien. D2D telah mengubah rangkaian tanpa wayar yang terkini dengan tren baharu kerana D2D dapat memainkan peranan penting dalam berkongsi sumber dengan memuatkan rangkaian di kawasan setempat dengan komunikasi langsung antara peranti dan berguna dalam bencana alam di mana BS dimusnahkan. D2D telah merevolusikan komunikasi langsung kerana ia adalah asas untuk rangkaian 5G. D2D membenarkan peranti miniatur seperti telefon bimbit, tablet, peranti radio berfungsi sebagai Relay Tidak Transparan (NTR) di mana mereka dapat menyediakan perkhidmatan serta lalu lintas ke hadapan, meminta perkhidmatan dengan komunikasi langsung tanpa memerlukan Stesen Pangkalan (SP) atau pusat infrastruktur rangkaian. Multi-hop D2D dapat digunakan untuk komunikasi rakan sebaya atau bahkan akses ke rangkaian selular. Konsep komunikasi multihop D2D ini telah memperkenalkan sejumlah masalah dan cabaran yang tidak lazim berlaku dalam komunikasi selular semasa tradisional. Salah satu masalah utama dalam D2D adalah keselamatan yang diperlukan dalam komunikasi D2D untuk menghantar maklumat dengan selamat melalui saluran yang tidak selamat. Cabaran utama ketika mempertimbangkan keselamatan adalah bahawa teknik keselamatan yang ada saat ini tidak dapat diubahsuai kerana peranti yang

memerlukan keselamatan adalah miniatur dengan pemprosesan dan penyimpanan terhadap atau dibatasi oleh masalah kuasa dan lebar jalur. Masalah lain ialah bagaimana peranti dapat mendapatkan pengesahan bersama yang selamat untuk komunikasi yang selamat. Untuk mengatasi masalah ini, skema pengesahan multifaktor ringan yang membolehkan komunikasi selamat multihop melalui saluran terbuka dirancang dipanggil sebagai Protokol Pengesahan Multifaktor Berbasis ECC Ringan (LEMAP) dalam komunikasi D2D multihop. Analisis skema secara formal dilakukan dengan menggunakan kaedah BAN Logic yang terkenal yang digunakan untuk memeriksa kebenaran protokol. Analisis formal LEMAP membuktikan bahawa ia dapat mengurangi serangan ulangan, serangan Man-in-the-Middle (MITM), serangan perangkat rouge, serangan Denial of Service (DoS), serangan eksploitasi cap waktu, serangan peniruan dan serangan penyamaran. LEMAP juga mencapai kerahsiaan, integriti, privasi, penolakan, pengesahan bersama yang selamat dan tanpa nama. Kos komunikasi dan overhead komputasi juga dikira protokol penanda aras dan skema LEMAP yang dicadangkan. Hasil kajian menunjukkan bahawa LEMAP adalah 6 hingga 28 peratus lebih kuat daripada algoritma penanda aras yang dipilih seperti 2PAKEP, pengesahan berasaskan Chaotic dan protokol pengesahan TwoFactor. Selain itu, LEMAP memberikan keselamatan tambahan dengan menggunakan pengesahan kepercayaan, hash berganda, dan overhead pengesahan yang dikurangkan. Analisis logaritma diskrit menunjukkan bahawa LEMAP selamat daripada algoritma keselamatan semasa dan juga serangan kuantum. LEMAP adalah skema ringan dan fleksibel yang dapat digunakan dalam komunikasi 5G dan multihop D2D untuk menyediakan persekitaran komunikasi yang selamat.

Kata kunci: Keselamatan D2D, keselamatan D2D multihop, multi factor, keselamatan ringan, ECC

TABLE OF CONTENTS

	Page
DECLARATION	i
DEDICATION	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	v
<i>ABSTRAK</i>	vii
TABLE OF CONTENTS	ix
LIST OF TABLES	xvi
LIST OF FIGURES	xvii
LIST OF ABBREVIATIONS	xix
CHAPTER 1: INTRODUCTION	1
1.1 Research Background	1
1.2 Problem Statement and Research Challenges	6
1.3 Idea and Motivation	9
1.4 Research Objectives	9
1.5 Scope of Work	11
1.6 Thesis Contributions	11
1.7 Thesis Organization	12

CHAPTER 2: LITERATURE REVIEW	14
2.1 Introduction	14
2.2 Device to Device Communication	15
2.2.1 D2D Communication Modes	17
2.2.1 D2D Components	22
2.3 Security Requirements of D2D Protocols	24
2.3.1 Confidentiality	25
2.3.2 Integrity	25
2.3.3 Availability	25
2.3.4 Non-repudiation	26
2.3.5 Mutual Authentication	26
2.3.6 Anonymity	26
2.4 Security Challenges in D2D	26
2.5 Security Threats in D2D	29
2.5.1 Single hop Challenges	29
2.5.2 Multi-hop Challenges	32
2.6 BAN Logic	34
2.6.1 Extension by Sufatrio and Roland	36
2.7 Simulation Software	37
2.8 Current Approaches	38

2.8.1	Chaotic Map-Based Anonymous User Authentication Scheme	38
2.8.2	2PAKEP Security Scheme	40
2.8.3	Two Factor Security Scheme	43
2.9	Analysis Method	47
2.10	Summary	47
CHAPTER 3: SYSTEM DESIGN FOR LEMAP SCHEME		49
3.1	Introduction	49
3.2	System Model	50
3.2.1	Multi Factor Authentication Layer	50
3.2.2	Security Layer	51
3.2.3	LEMAP for D2D Multi-hop Communication	52
3.2.4	Notations Table for LEMAP (NTL)	52
3.2.5	Factors Attacks Mitigation Table for LEMAP (FMT)	55
3.3	System Design for LEMAP	57
3.3.1	Authentication Request Message (D1- CH)	58
3.3.2	Authentication Request Message (CH- eNB)	60
3.3.3	Authentication Response Message (eNB- CH)	62
3.3.4	Authentication Request Message (CH- eNB)	63
3.3.5	Authentication Response Message	65
3.3.6	Authentication Response Message	67

3.3.7	Authentication Response Message	68
3.3.8	The Authentication Request Message	70
3.3.9	Auth-Request Message	72
3.3.10	Authentication Request Message	73
3.3.11	Authentication Response Message	75
3.3.12	Authentication Response Message	77
3.3.13	Authentication Response Message (CH-D ₂)	79
3.4	Network Model	81
3.5	Performance Analysis	83
3.5.1	Formal Analysis	83
3.5.2	Communication Cost	87
3.5.3	Mathematical Analysis	88
3.6	Summary	90
CHAPTER 4:	RESULT AND ANALYSIS	91
4.1	Introduction	91
4.2	Development of LEMAP Protocol	91
4.3	Formal Analysis	112
4.4	Analysis of LEMAP Protocol	116
4.4.1	Authentication Goals	117
4.4.2	Assumptions	118

4.4.3	Idealization of Authentication Request Message (D1-CH)	119
4.4.4	Idealization of Authentication Request Message (CH-eNB)	121
4.4.5	Idealization of Authentication Response Message (eNB-CH)	123
4.4.6	Idealization of Authentication Request Message (CH-eNB)	125
4.4.7	Idealization of Authentication Response Message (eNB-CH)	127
4.4.8	Idealization of Authentication Response Message (CH-D ₁)	129
4.4.9	Idealization of Authentication Response Message (CH-D ₂)	131
4.4.10	Idealization of Authentication Request Message (D1-CH)	133
4.4.11	Idealization of Authentication Request Message (D2-CH)	135
4.4.12	Idealization of Authentication Request Message (CH-eNB)	137
4.4.13	Idealization of Authentication Response Message (eNB-CH)	138
4.4.14	Idealization of Authentication Response Message (CH-D ₁)	140
4.4.15	Idealization of Authentication Response Message (CH-D ₂)	142
4.5	Mathematical Analysis	144
4.5.1	Total Communication Cost	145
4.5.2	Computational Overhead	159
4.5.3	Authentication Overhead	161
4.6	Simulation Analysis of LEMAP Protocol	163
4.6.1	Packet Delivery Ratio without Attacker	166
4.6.2	Packet Delivery Ratio with Attacker	167

4.6.3	Effect of Packet Overhead	169
4.6.4	Comparison of Processing Time	171
4.6.5	Effect of Increasing Rogue Relay Station	172
4.6.6	Discussion on Computational Security Analysis	174
4.7	Security Analysis	175
4.7.1	Brute Force Attack	175
4.7.2	Pollard's Rho Method	176
4.7.3	Baby Step Giant Step	177
4.7.4	Keyspace	177
4.7.5	Key size	177
4.7.6	Processing Cost	178
4.8	Verification of Security Requirements	181
4.8.1	Data Confidentiality	181
4.8.2	Data Integrity	182
4.8.3	User Privacy	182
4.8.4	Traceability	182
4.8.5	Non-repudiation	183
4.8.6	Mutual Authentication and Key Agreement	183
4.9	Summary	183

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS	185
5.1 Introduction	185
5.2 Significant Contribution of LEMAP	186
5.2.1 Privacy	187
5.2.2 Integrity and Confidentiality	187
5.2.3 Non-Repudiation	188
5.2.4 Multi-factor Authentication	188
5.2.5 Authentication Overhead	188
5.2.6 Formal Validation	189
5.2.7 Quantum Attack Safe	190
5.3 Future Work	191
REFERENCES	192

LIST OF TABLES

	Page
Table 2.1 Description of D2D Components	23
Table 2.2 Attacks Mitigated by Protocols	46
Table 3.1 Notations Table for LEMAP	53
Table 3.2 Factors Attacks Mitigation Table for LEMAP (FMT)	56
Table 4.1 BAN Logic Messages Interpretations	113
Table 4.2 Total Communication Overhead	160
Table 4.3 Device / Relaying Node Computational Parameters	164
Table 4.4 Message Sizes Declaration of Different Message Parts	165

LIST OF FIGURES

	Page
Figure 2.1 Modes of D2D Communication	18
Figure 2.2 Basic Multi-hop D2D Communication	19
Figure 2.3 Scenario of Direct Communication	20
Figure 2.4 Out of Coverage Communication	21
Figure 2.5 D2D Cellular Model	24
Figure 2.6 Replay Attack	30
Figure 2.7 Man in the Middle Attack	32
Figure 2.8 Chaotic Timing Diagram	41
Figure 2.9 2PAKEP Timing Diagram	43
Figure 2.10 TwoFactor Timing Diagram	45
Figure 3.1 System Model of LEMAP	50
Figure 3.2 Network Model LEMAP Scheme	83
Figure 4.1 Authentication Request Message at D1	93
Figure 4.2 Authentication Request Message at CH	94
Figure 4.3 Authentication Challenge Response Message at eNB	96
Figure 4.4 Authentication Challenge Response Message at CH	98
Figure 4.5 Authentication Challenge Response Message	100
Figure 4.6 Authentication Challenge Response Message for CH	102
Figure 4.7 Authentication Challenge Request Message at D1	103
Figure 4.8 Authentication Challenge Request Message at D2	105
Figure 4.9 Authentication Request Message for D1 & D2	106
Figure 4.10 Authentication Response Message at eNB	108
Figure 4.11 Authentication Response Message at CH	110

Figure 4.12	LEMAP Timing Diagram with Messages Flow	111
Figure 4.13	Effect of Increasing Hops on Computational Cost	161
Figure 4.14	Authentication Overhead with Multi-hop	162
Figure 4.15	Simulation Setup of LEMAP and other Benchmarking Protocols	163
Figure 4.16	PDR without Attacker for Proposed and Benchmarking Protocols	167
Figure 4.17	PDR with Attacker for Proposed and Benchmarking Protocols	168
Figure 4.18	PO without Attacker for Proposed and Benchmarking Protocols	170
Figure 4.19	PO with Attacker for Proposed and Benchmarking Protocols	171
Figure 4.20	Processing Time for Proposed and Benchmarking Protocols	172
Figure 4.21	Effect of Increasing Rogue Relays in terms of Traffic Simulation	173
Figure 4.22	Ratio of Computational Cost	181

LIST OF ABBREVIATIONS

3G	Third Generation Cellular Communication
4G	Fourth Generation Cellular Communication
4G LTE	Fourth Generation Long Term Evolution
4G LTE-A	Fourth Generation Long Term Evolution Advanced
5G	Fifth Generation Cellular Communication
AES	Advance Encryption Standard
AP	Access Point
Auth	Authentication
BAN Logic	Burrows, Abadi and Needham Logic
BFA	Brute Force Attack
BFC	Blind Fold Challenge
BS	Base Station
BsGs	Baby Step, Giant Step
CA	Certification Authority
C_{dev}	Communication Devices
CU	Cellular Users
ECC	Elliptic Curve Cryptography
Ch	Challenge Scheme
CH	Cluster Head
CN	Core Network
D2D	Device to Device Communication
DES	Digital Encryption Standard

DH	Diffie Hellman
D ₁	Device with ID 1
D ₂	Device with ID 2
DLP	Discrete Logarithm Problem
DoS	Denial of Service
DDOS	Distributed Denial of Service
DT	Trudy Device
ECC	Elliptic Curve Cryptography
ECDH	Elliptic curve Cryptography with Diffie Hellman
eNB	Evolved Node B
E-UTRA	Evolved Universal Terrestrial Radio Access
f _i	Share frequency
GW	GateWay
IoT	Internet of Thing
LTE	Long Term Evolution
LEMAP	Lightweight ECC based Multifactor Authentication Protocol
MANET	Mobile Adhoc Networking
MAC	Medium Access Control
MITM	Man in the Middle Attack
M-MIMO	Massive Multiple Input Multiple Output
MRBS	Master Relay Base Station
MFA	Multi Factor Authentication
NIST	National Institute of Standards and Technology
NTR	Non-Transparent Relay

OTP	One Time Password
P _B	Device B Public Key
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
ProSe	Proximity Based Services
QoS	Quality of Service
RDp	Reactive Discovery Protocol
Req	Request
Resp	Response
RSA	River Shamir Adleman
SHA v3	Secure Hashing Algorithm Version 3
SP	Secret Point
SRP	Secure Routing Protocol
SK	Secret Key
ts	Timestamp
UE	User Equipment
WIFI	Wireless Fidelity

CHAPTER 1

INTRODUCTION

1.1 Research Background

Increase in cellular devices and demand for higher and fast data rate has put forward research and evolved Fourth Generation (4G) Long Term Evolution (LTE) towards Fifth Generation 5G (Alsharif & Nordin, 2017). Device-to-device (D2D) communication is a transmission in which devices directly communicate with each other without an intermediate device. It helps in expansion of cell coverage and increases frequency reuse in a 5G network. D2D communication is a core technology of 5G communication and adopts approach to facilitate work without centralized control mechanism to provide wireless network more spectrum and energy efficient with traffic offloading. 5G-D2D technology promises to improve current technologies by providing a proficient and reliable strategies for efficient resource utilization solutions to meet increased demand for future high network performance.

D2D apportions cellular traffic to offload from network-centric cellular links to peer-to-peer (P2P) wireless systems enabling low computational devices to take partial decisions besides increase in data rate, coverage and network-capacity (Li et al., 2018; Lee et al., 2016). It permits the communication to happen under the presence of infrastructure called as network assisted or without network assistance (Liu et al., 2015) but in any case, the devices must be registered first to a cellular network to start the provision of services. D2D utilizes the direct link between user equipment's (UE) to soften the load on cellular link such as base station (BS) thus empowering the user devices to act as an intelligent authorization and data dissemination devices (Ahmad et al., 2017, Gandotra & Jha, 2016). However, typical D2D

communication in 4G has various security challenges including impersonation, man in the middle (MITM), replay, eavesdropping, privacy, and denial of service (DOS) attacks etc. When devices are allowed to work as intelligent relays and authorization, this has exposed devices communication to several security loopholes and breaches for instance: quantum attacks, 51% attacks, MITM attack, masquerading attack, DoS attack, rouge relay attack and privacy issues in current cellular network settings (Cheng et al., 2017; Haus et al., 2017; Habib et al., 2017). These security challenges are more crucial and harder to mitigate because of the resource-constrained nature of cellular devices. Therefore, there is an immense need to consider security design requirement for ensuring secure and trustworthy environment for D2D cellular communication. To solve these security challenges in D2D communication, a lightweight and secure D2D communication system is required that can provide secure mutual authentication, data confidentiality/integrity and anonymity.

D2D communication is an integral part of 5G and is based on LTE (Kato, 2016) and uses proximity services to communicate between devices and share data without the need for authorization by central device. D2D even can provide services with low signal strength or even no coverage and is a big relief for area with weak infrastructure. D2D communication provides fast data rate as there is no need to request services from the central network (Gandotra & Jha, 2016). Evolution of wireless networks and Internet of Things (IoT) have convinced network operators to support D2D and provision of D2D especially in LTE (Astely et al., 2013). D2D communication using proximity services not only reduces communication cost but also provides higher data rate and reusability. D2D also permits sharing of resources such as spectrum, power application, services, data and social contents for any number of users that are near the proximity range forming a base for mobile cloud computing (Ghudayyer et al., 2017; Tehrani & Yanikomeroglu, 2014).

There are several D2D applications such as local communication where multiple devices can communicate with each other to provide services like social data services, local address services and cellular data offloading. These days, one of the common D2D applications is IoT communication where multiple devices can be connected to each other using wireless network and provide data related to home, offices, vehicles, and emergency services. With IoT provisioning, a single device can collect all sensor traffic as one unit and then forwards this to BS. One of the major applications of D2D is emergency communication services where even with weak network or no coverage, mobile devices can be connected to form a network and help the restoration and rescue operations. D2D can be similarly used for coverage extension without the need for installation of expensive BS. Also, the spectrum sharing and re-usage in one area, massive multiple input and multiple output (M-MIMO) are few of the applications (Liu et al., 2015; Wei et al., 2014). With the provision of devices to provide services, data, applications and spectrum sharing gives rise to vulnerability in terms of security and trust.

For D2D communication, each device is referred as user equipment (UE) or devices in literature but in this study, the devices are referred to as devices. Each device communicates with the evolved Node B (eNB) to get the authorization if Base Transceiver Station (BTS) or mostly referred as the base station (BS) is not in range. eNB is an authorized small base station installed by cellular companies having enough resources and a direct link to allow D2D communication and authorization. The devices that receive authorization from eNB or BS can communicate directly with each other (Lien et al., 2016; Raghothaman et al., 2013). The security and device validation must be established before communication between two devices as any compromise can result in all major security attacks possible that

were even non-existent before the D2D technology (Haus et al., 2017; Tehrani & Yanikomeroglu, 2014).

Several algorithms have been proposed for D2D communication security. These algorithms include usage of asymmetric and combination of asymmetric and symmetric cryptographic algorithms such as Rivest Shamir Adleman (RSA) (Ometov et al., 2016; Olshannikova et al., 2016), Diffie Hellman (DH) (Sedidi & Kumar, 2016), Elliptic Curve Cryptography (ECC) (Javed et al., 2017), Elliptic Curve Cryptography with Diffie Hellman (ECDH) (Hossain & Hasan, 2017; Yao et al., 2016) or some other combinations have also been used. In most of these techniques, BS serves as a certification authority (CA) for initial registration of devices. Once the devices are registered with the CA, they hold their public and private key pair for communication through which devices send secure message for authorization to secure communication to eNB or CA. The receiving eNB then checks the nearby devices and sends the authorized request to neighboring devices as well as authorized response to requesting devices. Each device must be authorized before communication. Once the authorization is done then communication can occur through the same asymmetric or mostly symmetric algorithm such as Advanced Encryption Standard (AES) or Digital Encryption Standard (DES).

The security layer of D2D is still at infancy and doesn't address all security challenges and attacks. Authorization of devices is one of the key challenges that usually is addressed by strict security classification of behavior (Wong, 2017). Authorization of devices is performed through eNB based message verification that requires each device to authenticate before any communication and thus requires additional authorization messages before communication (Habiba & Hossain, 2018; Nasrallah et al., 2018).

Usually the security is achieved by having a larger key size but it requires higher computational power and higher space (Othmen et al., 2017). Devices in D2D communication have limited computation and limited space and thus cannot have higher operational and computational cost (Hu et al., 2003). Authors have addressed security issues as D2D communication is over open non-secure channel. Privacy issues are also addressed by many researchers that keep secrecy of user when communication occur through eNB. Thus many schemes have been proposed to handle security issues like MITM, DoS and masquerading attacks especially to focus on single attack mitigation (Javed & Khan, 2019; Javed et al., 2019; Khan et al., 2017).

Multi-hop communication requires a new class of security algorithm as it results in newer attacks such as rogue relay and 51% attack (Gupta et al., 2018; Javed et al., 2017). Some of the solution provided use pseudo identity for each user but require eNB to provide the pseudo identity at time of each communication (Zhang & Shen, 2015). Collaboration and cooperation are key in D2D network which require device validation that must be established before starting communication. Validating the trust has been addressed by number of authors (Tata & Kadoch, 2014; Imai et al., 2006) but adaptive techniques are required to handle mix behavior of the devices that is acting partially as malicious and in some cases as selfish (Melki et al., 2016; Qin et al., 2016; Kim & Han, 2012).

This research mainly focuses on identifying security challenges associated with D2D communication by designing a lightweight and trustworthy security scheme which can mitigate above mentioned attacks with low authentication overhead, reduced computation cost as well as lower communication cost. The proposed scheme is based on Elliptic Curve Cryptography (ECC) which is one of light weight asymmetric-key technique compared to

currently adapted public-key encryption algorithms such as RSA. ECC provides 3072-bit of RSA cryptographic security using a 256-bit key.

1.2 Problem Statement and Research Challenges

Multi-hop D2D communication has several challenges. One of the major constraints is the lack of secure channel that leads towards several attacks specifically DoS, replay attack, MITM attack and identity reveal attacks. Many other challenges also exist like privacy issues, frequency hopping (Adam et al., 2019), network coding (Huang et al., 2019; Vanganuru et al. 2012), interface management (Tuan et al., 2019; Droste et al., 2015), network pairing (He et al., 2019), device discovery (Kaleem et al., 2019; Doppler et al., 2011), device security and trust (Javed et al., 2017; Company, 2003).

In multi-hop D2D communication, device and information security is a key challenge which can destroy the whole communication if compromised. Although current security schemes have addressed some of challenges, yet a number of challenges require further attention. One of the challenges is that key size must be small as larger key size results in higher operational cost. Normally, larger key size is required to make security scheme safer against quantum attack but this results in higher operational cost. Researches have shown that a very large key size cannot be used in D2D security scheme due to memory, storage and computation requirements (Javed et al., 2017; Wang et al., 2017; Zhang et al., 2017).

Most of the authors focused on mitigating well-known and common MAC Access Control (MAC) layer attacks such as Replay attack, MITM, DoS attacks and impersonation attacks. This research is based on primitive assumptions such as identity can be shared publicly, communication channels are always secure, some of the credentials can be sent without encryption, timestamp cannot be modified, single hashing can resolve the integrity

problem and cryptosystem is free of quantum brute force and password guessing attacks. However, several researchers believe that the discussed assumptions are not addressed carefully and it can provide space to common MAC layer attacks. For instance, identity reveal attack can lead to theft of identity which further leads towards impersonation attack or MITM attack.

As compared to normal cellular services, D2D communication offers high authentication overhead because numerous messages are exchanged for registration and mutual authentication. In order to complete authorization, devices must be verified and validated by Cluster Head or eNB and get authorization before starting actual communication (Habib et al., 2017; Hossain & Hasan, 2017; Wang et al., 2017; Ramadan et al., 2016; Yao et al., 2016; Zhang et al., 2016). In this whole authorization process, many messages are exchanged for communication which not only increase authentication overhead but also increase communication cost.

Privacy is another big issue in D2D communication as D2D is based on proximity services. In proximity services, real identity and location of devices is not hidden so the real identity and location of devices is apparent to other devices that is not desired by most of the devices. The real identity of devices should be hidden to maintain their privacy and real identity details. If a real identity of device is compromised, a communication pattern can be established which can also result in finding identity of any devices participating in communication even if the channel is secure (Hsu et al., 2017; Wang et al., 2017; Ramadan et al., 2016).

D2D allows communication directly between two devices which is referred as single hop communication. All this communication usually occurs on non-secure channel while the devices can be semi or non-trustworthy for the communication.

In multi-hop communication, a number of attacks such as Replay attack, Denial of Service (DoS) or Distributed Denial of Service (DDoS), Man in the Middle (MITM) and Identity Reveal attacks can occur (Haus et al., 2017; Javed et al., 2017; Wang et al., 2017; Zhang et al., 2017; Sedidi & Kumar, 2016; Zhang et al., 2016; Liu et al., 2015). This can also result in impersonation attack and masquerading attack where false devices can claim as real one (Ji et al., 2016; Nomikos et al., 2014). Replay attack is performed by repetitive delivery of a message sent by an adversary (Haddad et al., 2015). Attack on confidentiality will result in leakage of all sensitive information and may also result in compromised integrity (Khan et al., 2017; Wang et al., 2017; Zhang et al., 2017; Zhang et al., 2016; Ometov et al., 2015). D2D devices can act as intelligent relays where the devices can decode and forward the whole traffic that can make it vulnerable to already discussed attacks.

Literature shows a very limited work in area of threat mitigation of multi-hop communication and usually focuses on identification of security challenges (Nardini et al., 2017). Current schemes focus on mitigation of either one or two or a few of the security attacks, mostly focusing on MITM attack; whereas a comprehensive scheme that can mitigate most of security challenges at once is missing (Khan et al., 2017; Shen et al., 2016). Few techniques that have tried to address this challenge resulted in additional computation and authentication overhead on small miniature devices which have already limited computation and storage, as these devices are mostly in the form of mobile phones, tablets

and other hand-held devices. Thus a comprehensive security scheme must address this issue (Javed & Khan, 2017; Javed et al., 2017; Khan et al., 2017).

Most of the authors achieved secure end to end communication at the expense of high computation cost and message authentication overhead in multi-hop scenario. However, it is well agreed that using lightweight security mechanism and transmitting a small number of messages over communication link are always desirable as well as reducing the challenges of security threats, authentication overhead, communication and computation cost which should be feasible for miniaturized devices.

1.3 Idea and Motivation

D2D communication is an integral part of LTE-Advance (LTE-A) and 5G (Khan et al., 2018) where data availability and data rate must be higher with the lowest latency. The usage of public devices to act as authorization devices or decode and forward devices have resulted in several security issues such as DoS attacks, Rogue Relay attacks and MITM attacks which were not possible in earlier form of cellular communication. The motivation behind designing such a security algorithm is that numerous researchers conducted research in designing such a security scheme but most of the security algorithms have either unrealistic assumptions or do not address all security requirements simultaneously. As D2D promises number of applications that are necessary for high speed and low latency communication in 5G, it can be only possible if a lightweight secure environment can be created.

1.4 Research Objectives

This research mainly focuses on contriving a secure and lightweight algorithm for a multi-hop D2D communication that can satisfy all major identified security requirements.

This research designs a lightweight security algorithm called Lightweight ECC based Multifactor Authentication Protocol (LEMAP). Especially, the following research objectives are addressed in this research:

- i. To identify and investigate security challenges in existing D2D communication network.
- ii. To develop:
 - a. Lightweight ECC based Multifactor Authentication Protocol (LEMAP) that has secure end-to-end communication and reduced authentication and computation overhead.
 - b. A certificate-less secure lightweight multi-hop D2D communication scheme for mitigating above mentioned security challenges.
 - c. To evaluate the network performance of the proposed scheme using NCTUns for packet overhead, packet delivery ratio, effects of increasing route cluster head and processing time.
- iii. To conduct the Formal Security Analysis for evaluation of the proposed Protocol.
- iv. To check correctness and validation of proposed protocol using formal methods and non-formal security conformity methods against set of given attacks.
- v. Performance evaluation of proposed protocol through communication cost, authentication overhead and computation overhead and Quantum attack safety using discrete logarithm problem.

1.5 Scope of Work

To accomplish above mentioned objectives, the scope of the study covers that the research work assumes two devices are connected to eNB where Cluster Head (CH) works as a relay device. Cryptographic technique Elliptic Curve Cryptography (ECC) is used to provide lightweight security. Multi-factor authentication is achieved using onetime password (OTP), timestamp is used for message freshness, integrity of messages is ensured using Secure Hashing Algorithm version 3 (SHA v3) and simple Blind Fold Challenge (BFC) is used for mutual authentication.

This study identifies and investigates security challenges in D2D such as MITM, Replay, Identity Reveal, Rogue Relay, DoS, Masquerading and Quantum attacks. To evaluate efficiency and performance of the proposed scheme, computational overhead is computed using computation time and Capkun equation is used to estimate communication overhead. Security analysis is performed using Pollard Rho methods. The validity and correctness of the scheme is evaluated using Burrows–Abadi–Needham (BAN) logic, a formal analysis scheme.

1.6 Thesis Contributions

There are number of contributions in this research dissertation which are listed below:

The first contribution is a lightweight cryptographic multi-factor authentication scheme that helps secure D2D communication in an open insecure environment. This is a novel cryptosystem that utilizes ECC with Elgamal for achieving confidentiality, integrity, and non-repudiation. Elgamal has a smaller key size which helps not only in reduction of operational and communication cost but also makes it usable on small miniature devices.

Usage of Elgamal helps in achieving asymmetric key exchange that is one of the key requirements in open and mobile environment. It also applies digital signature to achieve authentication while double hashing using SHAv3 combined with timestamp and blind fold challenge scheme provides three-dimensional security that is integrity, freshness, and mutual authentication.

Three-dimensional security using Double Hashing based on SHAv3 combined with multi-factor authentication provides integrity, confusion, diffusion, freshness and mutual authentication. Multi-factors used for authentication include onetime password OTP (Biometrics, random number), timestamps, challenge and password which provide mitigation of all major security attacks for complete secure communication. This scheme also offers reduced authentication overhead, communication and computation cost due to merged challenge-response scheme.

The proposed scheme enhances the security performance by addressing all security requirements. It reduces the authentication overhead for single hop and multi-hop communication. It has smaller computation overhead that helps devices to consume less computational power and has also lower communication overhead resulting in reduction of network traffic significantly.

1.7 Thesis Organization

The thesis comprises five chapters. The first chapter provides introduction to the thesis. The topics covered in the first chapter include research background, research challenges, problem statement, scope and importance of this research.

Chapter 2 discusses the security challenges of D2D communication and highlights the significance that D2D provides. Security requirements that are key for assessment of any security protocols are also highlighted. Security challenges for single hop and multi-hop such as MITM, replay, impersonation, identity reveal, rouge relay, DoS and masquerading threats are also identified. Current benchmark approaches are highlighted according to their workings. Analysis and verification techniques used in various research works are highlighted in this chapter.

Chapter 3 provides a detailed flow of LEMAP where only two devices are directly communicating but the communication must pass through multiple hops. This chapter also provides a detailed system design of two sub layers proposed as D2D security layer and MFA layer. The first layer is referred as Multi Factor Authentication (MFA) layer and second layer is referred as security level layer. Complete scheme details are explained in the section after system design. Analysis methods based on performance and computation are discussed at the end of the chapter along with formalization techniques used for validation and verification.

Chapter 4 provides verification of LEMAP and benchmarking using the formal analysis with BAN logic. The verification of LEMAP against security attacks is tested and performed and computational security is also verified using the mathematical proven security methods. The cost analysis of benchmarks and LEMAP is performed while in the last section, the simulation analysis of the proposed method is also performed.

In Chapter 5, the security requirements which are fulfilled by LEMAP are explained. The overall thesis is concluded with the details on significant contribution of this research. The future directions of this research are also outlined.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The newly evolved 5G cellular wireless network is developed to provide high speed data, broadband and multimedia services with lower latency and energy consumption for various mobile devices. To achieve higher data rate, technologies like D2D are integrated into 5G. D2D communication is one of the key technologies incorporated to enhance 5G performance (Hussein et al., 2020). D2D is a direct communication method that enables two devices to communicate directly with each other without involving infrastructures such as access points (AP) or BSs. Bluetooth and WiFi-Direct are the most popular D2D techniques which work on unlicensed bands but on the other hand, cellular networks do not support direct over-the-air communication between users and devices. However, with the emergence of 5G, high data rate consuming applications and fast growth of Machine-to-Machine (M2M) applications, D2D communication plays progressively important role. It facilitates the discovery of geographically close devices and enables direct communication between these neighboring devices which improves communication capability with high data rate. Moreover, it reduces power consumption and delay in communication.

Despite many advantages, still many challenges and threats exist related to D2D communication. This research focuses mainly on security issues of D2D, threats involved in D2D during communication and secure mutual authentication. In this research, multifactor based mutual authentication scheme is proposed to overcome security issues during communication. Correctness and validity of the proposed scheme is verified by using formal

method BAN Logic. Next section provides basics of D2D, the challenges associated with D2D and the related works that have been done in D2D security.

2.2 Device to Device Communication

Device to Device (D2D) communication is a major and integral part of LTE-A and 5G. Especially, in the next generation cellular network D2D will be a major role player as it ensures high data rate and low latency. The research on D2D has been drawing attention since last few years where academia and industry are working together to standardize the process (Gandotra et al., 2017; Wong, 2017; Gandotra & Jha, 2016; Noura & Nordin, 2016; Gupta & Jha, 2015). D2D allows communication with the neighborhood devices which can communicate directly, and both have infrastructural network eNB, Core Network (CN) and Access Point (AP). D2D communication has shown that it can reduce huge network load, manage power consumptions, enhance network coverage and boost up traffic as well as reduction in delays (Gandotra et al., 2017). In academia, the D2D is introduced and used in LTE-A network to enhance communication performance (Li et al., 2017). D2D communication can work even though there is partial or no involvement of network infrastructure which is making it more popular for usage in the disastrous areas or low coverage services area (Biswash et al., 2017).

D2D techniques such as Wi-Fi-Direct (Trifunovic et al., 2011), Bluetooth, short-range wireless are already popular and in place. However they work without involvement of cellular network for communication and operate as an independent network. Cellular network doesn't allow direct communication even in the area of the cell device that is a fundamental block of the cellular network (Grossglauser & Tse, 2002). To achieve the cellular network services in 5G and LTE-A, the complete architecture and infrastructure

need to be updated for effective communication. There are plenty of researches that have been conducted in this area and have focused in some areas such as mode selection (Jänis & Ribeiro 2010; Shirani, & Kossentini, 2000), allocation of resources (Phunchongharn et al., 2013; Zulhasnine et al., 2010), interference control (Gu, J., Bae et al., 2011; Jänis et al., 2009) and power control (Janis et al., 2009; Yu et al., 2009). Industrial researches have been in the area of D2D for development of protocols such as the introduction of FlashLin Q (Theobald et al., 2014; Baccelli et al., 2012) that is used for communication of two devices. The standardization of D2D is going on through the Third Generation Partnership Project (3GPP) (Shen et al., 2012).

Another important aspect of D2D is the proximity-based services (ProSe) that allows the devices to find its neighborhood or nearby devices (Ta et al., 2014; Yang et al., 2013). The study of ProSe is underway in LTE-A network and its system architecture and network functions have been made. Current researches are being underway to develop the security and discovery aspects as well as on radio services (Oueis et al., 2017; Ferrús & Sallent, 2014; Husain et al., 2014). D2D assumes that communication can only occur if the devices are in proximity area. Initially for D2D communication, the authorization happens at the network controller and then devices can communicate once the full trust is established. The basic function of ProSe is to develop the safety infrastructure for public and this feature was first released as LTE-R12. There are two important parts of ProSe range that are Device tier and Macro Cell tier. Device tier refers to ProSe area of device where the device can locate and communicate with nearby devices while Macro Cell Tier means that area of ProSe is of BS. The Macro Cell manages the complete list of the possible neighbor list. The Macro Cell tier is responsible for the communication of cellular-related services. On the other hand, device tier is used for D2D communication.

2.2.1 D2D Communication Modes

The communication mode selection is a very important aspect of D2D communication and is considered as a major challenge when conventional cellular network is combined with D2D communication. The mode selection is the technique that determines whether the traffic between two communicating devices is established via the central network, Base Station (BS) or D2D mode. The method of spectrum allocation is also determined by the mode selection. Depending on whether devices in close proximity communicate directly or not, and whether D2D users and devices use dedicated channels or reuse channels of cellular users (CUs), three basic communication modes for D2D systems exist which are cellular mode, dedicated mode and reuse mode (K. Doppler et al., 2010). In the cellular mode, D2D devices can communicate conventionally through Base Station and requires more resources than the D2D mode due to the long communication range. In the dedicated mode which is also known as overlay mode or device to device mode, D2D devices are assigned dedicated radio resources and a dedicated spectrum to establish a direct link between the devices. In the reuse mode, which is also referred to as underlay mode, D2D devices reuse the same radio resources with cellular devices and this mode utilizes the spectrum resources shared with other cellular devices to establish communication between the D2D devices. The mode selection has been studied by many researchers and several mode of selection methods have been proposed.

Figure 2.1: shows two major types of D2D communication that is Inband communication and Outband communication. Inband refers to licensed cellular frequencies or working under licensed frequencies that is a major part of the cellular network. Normal

network communication and D2D communication both work under the same licensed frequencies. Inband is more widely used as it provides a higher data rate and efficient utilization of frequencies (Asadi & Jacko., 2014; Asadi et al., 2014). Outband refers to the unlicensed frequencies in which different communication band is required and it is managed by devices itself. In Outband communication, data rate is quite low as compared to Inband. But it can use both D2D communication and cellular communication at the same time which requires extra computation and overhead (Asadi & Jacko, 2014; Asadi et al., 2014).

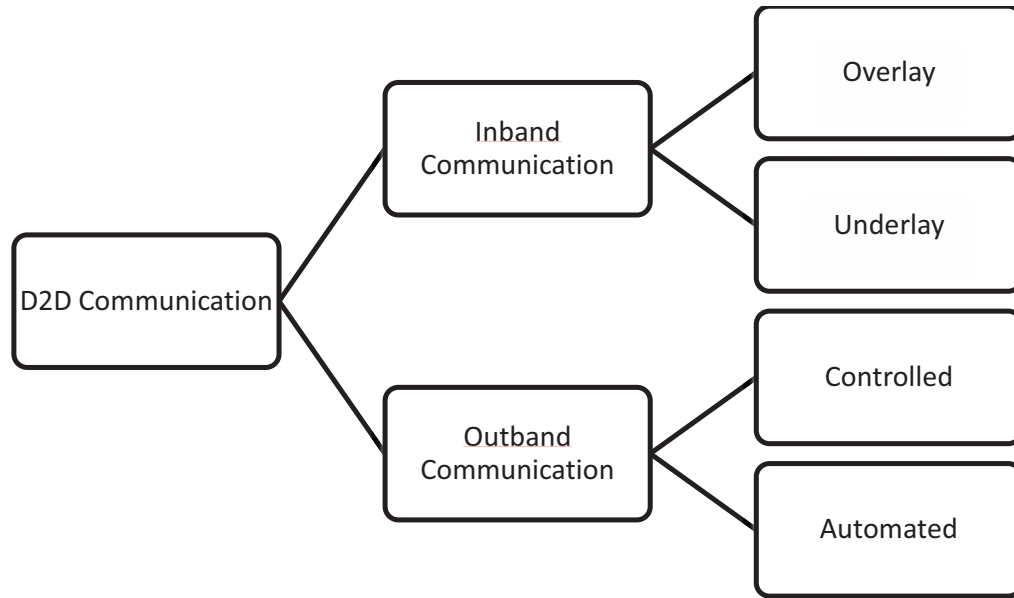


Figure 2.1: Modes of D2D Communication

Inband communication consists of Overlay and Underlay modes. In overlay mode different cellular band is used for communication while in underlay the same frequency band is used for cellular communication (Asadi & Jacko., 2014; Malandrino et al., 2014; Lin et al., 2013). Outband communication also consists of controlled and autonomous modes. In controlled transmission, the access point (AP) is serving as partial eNB and all communication take place through the trust established through the same cellular network.

In autonomous mode, communication occurs without AP or eNB and gives very low coverage enabling some devices to take hold of the transmission mostly in disastrous areas (Javed et al., 2019; Javed & Khan, 2019; Xu et al., 2012). Another important feature of D2D communication is soft handover which is possible even at local wireless communication level and provides an extended capacity about 5-10 Gbps between the devices. This was not possible in the current short-range free communication. The feature of handover is still in infancy and security is a big issue in D2D communication. Many researchers are focusing on this issue and proposing security algorithms to address it.

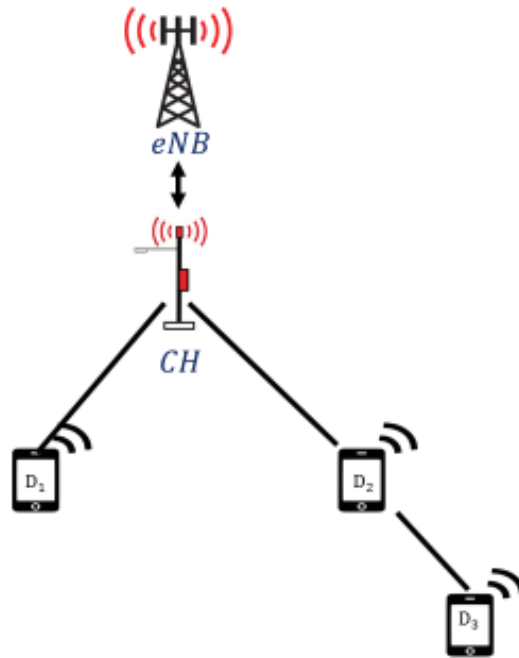


Figure 2.2: Basic Multi-hop D2D Communication

Figure 2.2 shows the multi-hop communication architecture of D2D that shows devices are controlled by eNB and devices can connect after establishing the authorization

and authentication with eNB. Cluster Head (CH) works as a relay agent for devices and provides services to devices in specific area. In recent trends, it is observed that D2D communication has achieved advanced features where multi-hop D2D communication is also possible. Multi-hop D2D communication will allow local area communication between multiple devices where one or more devices will act as relays for communication. Multi-hop D2D communication will also allow extended coverage so that device outside the coverage area can be accommodated.

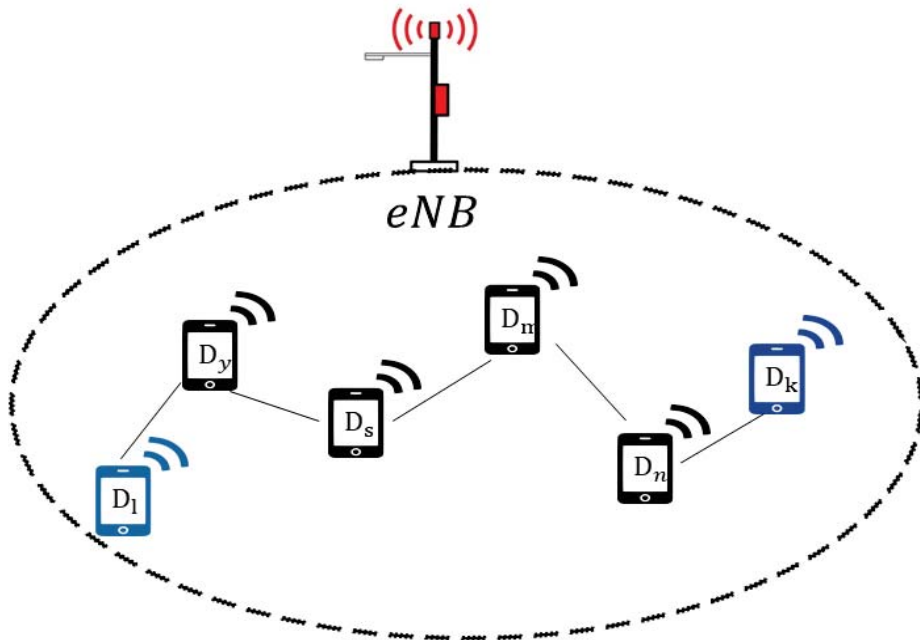


Figure 2.3: Scenario of Direct Communication

Figure 2.3 shows the scenario where devices are under the jurisdiction of eNB but would like to communicate directly after establishing successful trust. In this scenario, there are multiple devices as shown in Figure 2.3, however in terms of home setup or friend set up these devices have already established trust and would like to communicate directly by using relay devices (Tata & Kadoch, 2014; Imai et al., 2006). Figure 2.4 shows the scenario of multi-hop communication where some devices are out of the coverage range of eNB. This

scenario may arise in many cases such as disastrous area, non-cellular coverage areas or distant locations. To support the communication, the coverage to these devices can be provided if any of the registered devices is in range. This device will work as an acting eNB to those devices (Melki et al., 2016; Qin et al., 2016; Kim & Han, 2012). It is shown in (Nardini et al., 2017) that multi-hop communication must be done without boundaries and it supports a maximum coverage area without any geographical boundaries. This kind of communication will allow geo-fencing services to specific or multiple devices, in contrast to mobile-TV where everything is broadcasted in the cell. Integration of cellular network along with multi-hop network provides better Quality of Service (QoS) and flexibility. Another powerful feature is adaptability according to situations. There are several benefits associated with multi-hop D2D such as QoS, better data rate and network capacity.

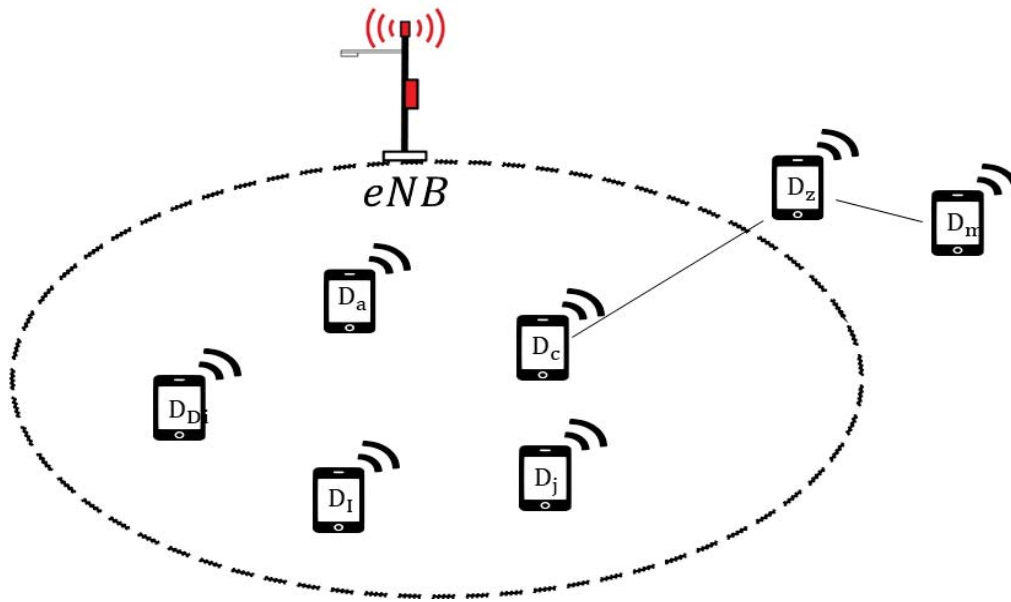


Figure 2.4: Out of Coverage Communication

QoS for devices in proximity is better since it has lower noise and signal to interference ratio as compared to traditional cellular networks. It is seen that multi-hop

results in the achievement of better QoS, but interference management must be made. In multi-hop D2D communication, higher modulation and available coding schemes result in saving bandwidth and high data rate due to small requirement of using channels to communicate to eNB. This results in two benefits as the same frequency for local communication can be used at full extent while main channel availability will result in a greater number of users, thus, increases network capacity. When communication will not be passing through the main cellular network and will be only used mostly for control message, it will result in reduction of great amount of network load. In case of partial or no network coverage, services will be available through the devices that are connected to the main network thus saving the cost of deployment of cellular systems and providing services in an area where the network cannot be deployed.

2.2.1 D2D Components

D2D components include devices, Cluster Head (CH) and eNB or Base Station. Each device must have been registered with the service provider through CH that acts as a gateway (GW) as shown in figure 2.5. Each device is assigned a unique pseudo-identity at the time of registration by eNB. Communication between devices takes place using these pseudo-identities. Each device works as decode and forward node to communicate with other devices. Initial registration is done through BS that broadcasts requests and allows verification. CH works as a forwarding device for specific area. Devices send requests to eNB through CH. eNB is a computationally powerful node that can manage all its underlying devices registration, authorization, verification, trust and all other data or service-related requests. Brief description of each component is given in Table 2.1.

Table 2.1: Description of D2D Components

Name	Description
BS	Base Station (BS) is a computationally powerful node that connects the local network to the core network. It performs routing control, internet provision, and all network related services. It manages eNB, verification and authorization control and also runs the proximity service control function that updates the neighbourhood information for devices (Tran, 2018).
eNB	eNB is an important part of Evolved Universal Terrestrial Radio Access (E-UTRA) in an LTE-A and 5G network. It performs authentication control for all devices and acts as security and interference control. It has high computational and storage resources and can manage parallel requests. It also broadcasts network membership and services to its members to manage the communication requests (Mach et al., 2018).
CH	Cluster Head (CH) is an intelligent forwarding device which serves a specific geographical area. It has low computational power and usually works as a forwarding device for all devices connected to the network. It forwards requests to eNB which manages authorization for all devices.
D_1, D_2	D_1, D_2 refer to devices that want to communicate with each other. D_1 sends communication request with D_2 to CH that forward it to eNB which can authorize both devices to communicate. It is a requirement that each device must be registered before becoming part of the area (Tran, 2018).

All the devices must trust CH and eNB, where eNB manages all the authorization, registration, re-authorization and communication control. It maintains the information table that contains all information about actual and pseudo identities of devices, its public key and neighboring information. The detailed explanation will be given in Chapter 3 in Section 3.3.3.

Figure 2.5 shows two devices D_1 and D_2 in a single cellular network which is managed by eNB. Devices are directly connected to CH in specific area which forward requests to eNB. Cluster Head works and manages device registration and handover for each area. Neighboring information is managed by Base Station (BS). The information that is shown in Figure 2.5 is based on infrastructural deployment of D2D.

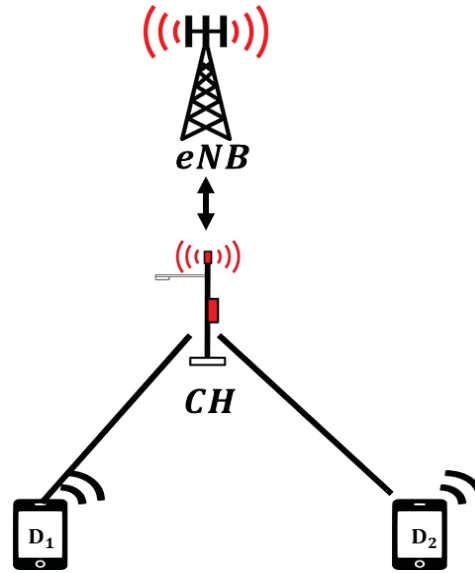


Figure 2.5: D2D Cellular Model

2.3 Security Requirements of D2D Protocols

In D2D communication, several security issues and threats still exist which have been identified in the literature. Many techniques have been proposed to overcome these threats.

These techniques cover some of the security requirements (Suo et al., 2012; Renauld et al., 2011; Fabian et al., 2010; Raya et al., 2006; Wallner et al., 1999). This section describes several security requirements for any D2D security protocols. These security requirements are generally for all types of communication either it is single hop or multi-hop network.

2.3.1 Confidentiality

The first security requirement is confidentiality which means data transmitted on open channel must be encrypted and only the intended recipient can decrypt and read it. To achieve confidentiality, a strong encryption scheme is required (Borgohain et al., 2015) to encrypt data so that it must be secure from adversaries during transmission.

2.3.2 Integrity

The second important security aspect is integrity which means when data is sent by the sender, it must be received to the recipient as it was sent. It means there is no tampering during transmission. To achieve integrity, a strong hashing technique must be applied (Li et al., 2014; Meister, 2013). After applying hashing, when recipient will receive data, its hash is checked and matched with actual message. If both are same, it means there is no tampering during transmission and hence data integrity is maintained.

2.3.3 Availability

Availability means services are available anywhere and at any time. In D2D communication, services should be accessible anytime and anywhere even under DoS or free-riding attacks (Lu et al., 2015). Free riding resistance refers that each UE must be registered as member of some eNB and have a unique identity. No free users can join the network until they register.

2.3.4 Non-repudiation

To ensure the reliability of the information transmitted, both parties must attach a private seal of a legitimate user as the basis for the information during communication. At the same time, this also makes it impossible for a sender to deny that one had not sent a message. Non-repudiation is achieved when none of the transmitting devices deny the sent message request. Digital signatures are used to achieve non- repudiation. Timestamps also help to document date and time when the message was sent which can help in achieving non-repudiation.

2.3.5 Mutual Authentication

To ensure a secure communication process between two devices, communicating parties must register with base station or central server and authenticate each other securely. In mutual authentication two devices authenticate each other before start of actual communication. Thus, the security scheme must offer secure mutual authentication.

2.3.6 Anonymity

Anonymity is a state in which somebody public identity is unknown or hidden. Anonymity must be achieved as participating communicating devices should not be recognizable by other communicating devices. To achieve anonymity, pseudo identity is used to protect the real identities (Hsu et al., 2017).

2.4 Security Challenges in D2D

There are many challenges that are associated with D2D communication like device design (Fodor et al., 2012), distance between UE, distance between BS and device (Wang & Chu, 2012), interference management (Shalmashi et al., 2013), device mobility management

(Zhang et al., 2017; Yilmaz et al., 2014), energy consumption (Jiang et al., 2015; Zhou , 2014) , spectrum usage and frequency selection (Monserrat et al., 2015; Sakr & Hossain, 2015), offloading techniques (Andreev et al., 2015). Resource allocation and resource management (Phunchongharn et al., 2016; Jiang et al., 2015) is one of major challenges due to its inherent limitations. Mode of D2D either licensed or unlicensed or another form such as Assisted or Un-Assisted makes it a challenge to support all modes (Asadi et al., 2014; Han et al., 2012). Security is a major challenge of D2D (Cheng et al., 2017; Haus et al., 2017; Habib et al., 2017; Hossain & Hasan, 2017; Javed et al., 2017; Wang et al., 2017; Zhang, 2017; Fujdiak, 2016; Li, 2016; Kato, 2016; Ramadan et al., 2016; Sedidi & Kumar, 2016; Yao et al., 2016; Zhang et al., 2016; Abd-Elrahman et al., 2015; Liu et al., 2015; Xi et al., 2014). Other aspects related to security are also identified in multiple types of research (Li et al., 2018; Ahmad et al., 2017; Lien et al., 2016; Kato, 2016; Tehrani & Yanikomeroglu, 2014; Raghothaman et al., 2013).

This research focuses on security and privacy issues that have appeared with the advent of D2D. Security solutions presented for LTE and cellular networks cannot address the issues that have arisen due to the inception of D2D. For instance, in LTE there is only mutual authentication between the users and main cellular network. Moreover, there is an agreement between users in the main cellular network. While in D2D, there is mutual authentication between the devices and similarly, key exchange after negotiation between devices also takes place. In the absence of security measures, the whole communication architecture can be compromised. There are a number of attacks that can occur either actively or passively (Zhang et al., 2017; Dholeshwar & Salapurkar, 2016; Wang et al., 2015; Wen et al., 2013; Jibi & Rakshanda, 2013). Some of the examples of most common attacks that are possible on D2D are eavesdropping attack, DoS, MITM attack, impersonation attack,

side channel attack, forge attack, free riding attack and rogue device attack. There are several privacy attacks or security issues that can be made successful in the current infrastructure of cellular network. Among those issues are privacy issues related to user identity privacy, location privacy, data privacy and unwanted messages.

Owing to the increased number of attacks on D2D communication, researchers in academia and industry have invested many efforts in designing secure communication algorithm. Research about D2D security is still at early stages. Some researchers used most widely used security algorithms for normal communication over network. A few researchers have used Mobile Adhoc Networks (MANETS) algorithms for proposing security solutions (Panaousis & Alpcan, 2014). Most of the security algorithms only focus on one or two security requirements that must be met for designing a secure technique for D2D. Another issue is that D2D designing is still under development and create an emerging security requirement issue. Some algorithms are proposed based on old requirements while a new requirement has emerged. Another issue is that devices involved in D2D have variable computation power and due to applications probability across different devices; any device can act as communicating device. Hence, the developed solution must consider a low computation device. Owing to this issue, many of the proposed solutions may be vulnerable to new era attacks (Yin et al., 2018; Aggarwal et al., 2017). Numerous techniques and approaches focused on secure data transfer, others focused on authentication and key agreements. These proposed techniques for D2D security usually focused on the security of data, sharing of data securely, authentication and agreement of keys. Most of the security techniques focus on single operator and security issues are considered individually without combining the security techniques with key management techniques. Research in D2D especially security in D2D is still at early stages and standardization has not been developed.

2.5 Security Threats in D2D

D2D inherently poses number of challenges and threats that can be categorized into single hop and multi-hop challenges.

2.5.1 Single hop Challenges

As discussed in previous section that D2D is more open to any kind of attacks that were even non-existent in traditional 4G and 4G-LTE network. But allowing the devices to act as relaying devices opens as a whole bunch of attacks that should be handled in a different way; as the devices have low computing power and are required to do number of new tasks which were not its actual part prior (Javed & Khan, 2019; Javed et al., 2019; Khan et al., 2017). The following is the list of attacks that can occur in a single-hop D2D communication.

2.5.1.1 Denial of Service Attack

In this type of attack, an attacker targets and sends huge traffic to a device or service and makes it inaccessible for legitimate users. An attacker can both flood the server or the IoT device with many fake requests and crash it due to resource constraints. This attack can be from one device or multiple devices. In D2D DoS attack, an attacker exploits the capabilities of eNB or BS by sending repeated delivery of false messages. DoS usually performed through replay attack that may result in stoppage of access to some service or complete resource (Javed & Khan, 2019; Javed et al., 2017).

2.5.1.2 Replay Attacks

The intruder can send intercepted message again and again or delaying message. Adding timestamp with message is a solution to avoid replay attacks because it ensures message freshness. During mutual authentication process, an adversary can intercept the

traffic and takes the message from legitimate node, later use this message after a certain amount of time and send to the base node to perform replay attack against base node (Hu & Evans, 2003). It is possible that adversary may not be able to decrypt the message, but it continues to send the message to BS or eNB that can result in DoS attack. If this attack is initiated from BS to sub-nodes or devices, this results in MITM attack. An example of attack is shown in Figure 2.6.

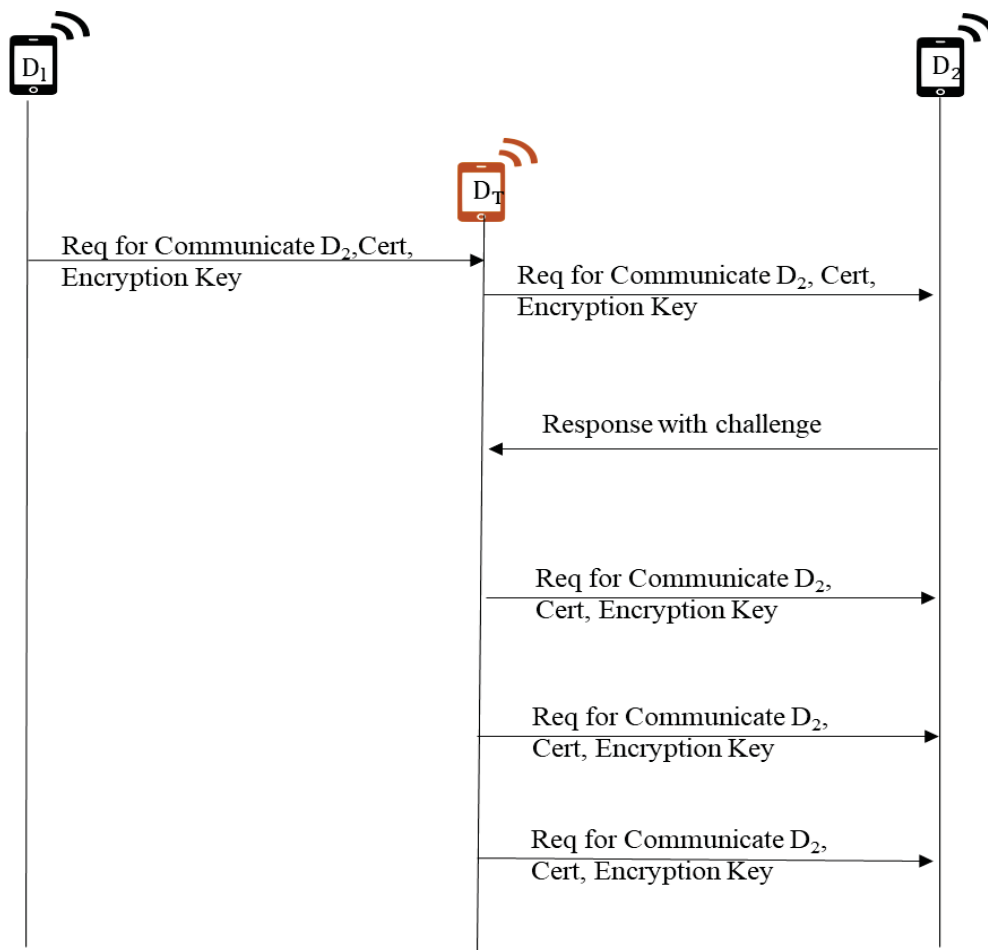


Figure 2.6: Replay Attack

2.5.1.3 Masquerading Attack

A masquerade attack uses a forged or fake identity of a legitimate device to gain unauthorized access to target device or network. Masquerade attacks are generally performed by stealing login credentials (IDs, Passwords) or by finding gaps in authentication process. If authentication process is not fully secure, it is highly vulnerable to masquerading attack. A masquerade attacker can be from inside network or from outside network as well.

In this kind of attack, one device pretends to be another device (Faria & Cheriton, 2006). This device can be a device acting as the Internet of things (IoT) or Master Relay Base Station (MRBS) or Non-transparent relay (NTR). This attack may happen by using two kinds of techniques; one is identity theft, and another is Rouge Base Station. If the identity theft is successful, then it will result in MITM attack and even if it not successful it will result in DoS attack (Khan et al., 2017; Javed et al., 2017).

2.5.1.4 MITM

MITM is a type of attack in which an adversary eavesdrop communication between two devices, intercepts the communication and starts conversation with devices. The legitimate devices cannot recognize either they are talking to legitimate device or an adversary. The main reason of MITM attack may be weak encryption, weak passwords or not using digital signatures in communication.

MITM attack is successful if encryption technique used is not too strong. In MITM, normally an attacker can decrypt the response messages successfully (Javed et al., 2019). The attack is illustrated in Figure 2.7 that shows two devices directly communicating while the attacker is listening to the whole communication. MITM attack is one of the most challenging attacks as it may result in whole communication compromise.

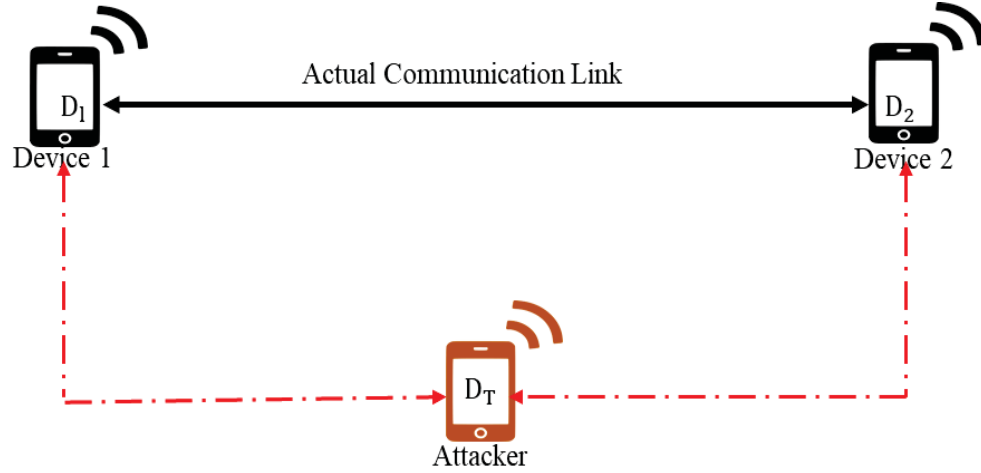


Figure 2.7: Man in the Middle Attack

2.5.2 Multi-hop Challenges

Multi-hop D2D communication introduces the following security attacks:

2.5.2.1 Rogue Device Attack

A rogue device is a device that is connected to your network without authorization. This type of device gets authorization due to lack of proper authorization rules in the network and can become a bot to launch DoS attack. Also a rogue device can be a sniffer which eavesdrop network and causes sensitive data theft, destruction of data, loss of services and can insert malicious data in the form of viruses, keylogging or pornography(Gupta et al., 2018; Javed et al., 2017).

2.5.2.2 Timestamp exploitation attack

Timestamp is used for message freshness which ensures that received message is fresh and within the time limit specified for that session. If the timestamp exceeds the time limit, the message is considered by an adversary and it is discarded. Sometimes an adversary intercepts the session within the specified time limit. This opens window for adversary to

initiate timestamp exploitation attack. In D2D communication, an adversary can intercept a message during specified timestamp to use it later.

2.5.2.3 51% Attack

The 51% attack occurs when several malicious devices supersede the number of legitimate devices. As most of the trust-based system relies on feedback from the devices, thus if the number of malicious devices is higher they can jeopardize the whole communication by giving false beliefs (Bastiaan, 2015).

2.5.2.4 Eavesdropping Attack

In an eavesdropping attack, an adversary sniffs network communication to gain unauthorized access to data, steal IDs information, modify or delete sensitive information. An adversary uses some software or application to sniff network communication and takes advantage of weak passwords, weak encryption, and weak privacy to steal information. Later adversary uses this private information to compromise nodes and degrade network performance. To avoid eavesdropping attack, strong encryption and authentication mechanism is required.

2.5.2.5 Pre-image Attack

In Pre-image attack, an attacker tries to find specific hash value of some message by using brute force attack. A cryptographic hash function should resist attacks on its preimage. To mitigate pre-image attack, double hashing technique is used. All the messages sent or received by one device to other, use double hashing digitally signed by the private key of the sender. Double hashing is a collision resolving technique in Open Addressed Hash tables. Double hashing uses the idea of applying a second hash function to key when a collision occurs.

2.5.2.6 Impersonation Attack

Impersonation attack is an attack in which an adversary adopts a fake identity of a legitimate device and starts communication with the target device. The target device cannot recognize either it is the legitimate device or the fake device.

2.6 BAN Logic

One of the famous techniques for formalization called as BAN logic is used for verification of proposed security algorithm called as LEMAP. The various inference rules are listed below; the lists above are the inference rules of the Burrows, Abadi, and Needham (BAN) Logic. There are many rules but below mentioned are used commonly. A detailed description of the rules can be found in (Sufatrio & Yap, 2008; Cohen, 2005).

First of the formalization techniques was made by Dolev and Yao for the security algorithms but their proposed methods have a restricted use due to complexity involved and lack of system details. Later, the Dolev and Yao introduced the capabilities model for attackers, and it was based on assumption that attackers can take control of the system resulting in wide usage of the protocol.

Still the proposed system had couple of limitations such as limitation of intruder was the restriction on usage of random number. Encryption and decryption were not part of the intruder system that resulted in in-complete attack. With this method any kind of weak security would have the same result as strong encryption.

One of the well-known computation model that was proposed was Bellare and Rogaway that was based on scenarios such as each attack must be made in scenario and is

played or executed like a game. The task is to create an algorithm where user cannot win after endless possibilities.

Burrows, Abadi and Needham algorithm, often referred as BAN logic is one the decent algorithms for checking the security of the system and still widely used for verification of security protocol using formal ways. BAN logic is based on symbols and can be used to perform attack analysis on security algorithms. It is based on rule that each goal means the authentication properties of security algorithm. It is also based on condition that algorithm is converted into definition and rules based on BAN logic principles.

Another condition is that security model must be identified before conversion. Next condition is to use the inferencing rule. Based on all these assumption, model and rules it is verified that security goal can be achieved or not. If it cannot be achieving, then the security protocol is vulnerable to attack and thus modification in algorithm is required else it passes the security test.

There are number of issues that were identified in BAN logic are that it doesn't handle the certification authority rules properly and it also cannot handle the Public key infrastructure (PKI) well. It also makes some assumption that might result into security weakness. In order to handle this an extension on BAN logic has been proposed. The extension in BAN logic resulted in the betterment of certification authority rules but made it complex.

One of the extensions in BAN logic is proposed by Sufatrio and Roland that handles few weaknesses such as goodness property of base station (BS) (Sufatrio & Yap, 2008; Cohen, 2005). The first issues identified by authors was the basic assumption on certificate trust as shown in Equation 2.1

$$\prod(K_{BS}^{-1}) \quad \text{Equation 2.1}$$

The assumption states that BS believes in Equation 2.1 as shown in Equation 2.2.

$$P \mid \equiv \prod(K_{BS}^{-1}) \quad \text{Equation 2.2}$$

Another issue that is identified is jurisdiction of message, it must be assumed that sender can send the message as he has jurisdiction as shown in Equation 2.3.

$$A \mid \equiv B \rightarrow BS(X, P) \quad \text{Equation 2.3}$$

where X is secret key and P is public key

The revocation of certification possibility can be introduced but it must be assumed that is missing in first that keys of CA are good and protected.

2.6.1 Extension by Sufatrio and Roland

To deal with identified issues, there were extensions proposed by authors.

2.6.1.1 For the idealization of certificates

It is assumed that certificate is fully signed by CA and it has good and secure secret key and public key pair. It removes the need of creating another message stream of trust between CA or BS and other nodes.

2.6.1.2 For the message Recipient

In order to make sure that message is sent by a correct recipient the message is signed using the private key of his own as shown in Equation 2.4

$$\prod(K_{BS}^{-1}, (BS(X, P))) \quad \text{Equation 2.4}$$

It ensures that the certificate is valid and can only be generated by CA. The goals for Device to Device(D2D) authentication protocols should be

$$D_B \models D_A \xleftrightarrow{K_{D(A,B)}} D_B \quad \text{Equation 2.5}$$

The above rule in Equation 2.5 says the device D_A believes that there is a secret key must be calculated without sharing between both devices D_A and D_B .

Similarly, the device D_{Ai} believes that there is a secret key must be calculated without sharing between both devices D_B and D_A . If the secret key $K_{D(A,B)}$ or SP is created and shared that key will be used as communication point for both devices as shown in Equation 2.6.

$$D_A \models D_B \models D_A \xleftrightarrow{K_{D(A,B)}} D_B \quad \text{Equation 2.6}$$

The message in BAN logic in extension are same as old one and thus all the old rules holds true along with trust.

2.7 Simulation Software

There are number of simulations software's that can be adapted for this research, out of which NS2, NS3, OPNET and NCTUns are one of the notable software. This research adapted a D2D communication of discrete even that why NCTUns is selected to be simulation software. It also provides implement IEEE802.16j protocol that helped this research in focusing on real implementation. NCTUns is high fidelity network simulator that can also work as emulator. Its an opensource platform that has integrated wireless network and VANET implementation that make it easier and more widely used among other

simulators. It also provides fast feedback look that helped this research in implementing sender and receiver messages among base station, devices, and head. This research also used Microsoft Excel to process the data logs received from NCTUns.

2.8 Current Approaches

Several approaches and techniques have been discussed in previous sections which can cover few security requirements and do not complete support for all the security requirements. Some of the research work that has been done used RSA, ECC, DH and other algorithms. This research selected three benchmark protocols based on their completeness, citations, standardization, and openness. Openness refers to the openness of algorithm along with its source code or easy to reproduce. The following three protocols explained are treated as a benchmark for this research.

2.8.1 Chaotic Map-Based Anonymous User Authentication Scheme

Chaotic Map-Based Authentication Scheme (Sandip Roy et al., 2018) is used for securing the data and perform D2D communication. The protocol uses an assumption that eNB is secure and trusted third party while two devices A and B want to communicate with each other. The device A will have to send a request to eNB for authentication to communicate with device B. The proposed scheme consists of registration phase and then authentication phase.

Firstly, registration phase is completed. In this phase, a user U_i gets his smart card SC from the medical Server S. Then communication between user U_i and Server S takes place on secure channel.

Secondly authentication phase starts. The user U_i selects its ID_i , password PW_i , biometrics B_i and 1024-bit random number b . Next by using fuzzy extractor generation procedure, U_i generates $(\alpha_i, \beta_i) = \text{Gen}(B_i)$, and computes masked password $RPW_i = H(H(ID_i || PW_i) || \alpha_i)$ and $C = H(H(ID_i || PW_i || b) || \alpha_i)$. Then U_i submits (ID_i, C) to server S via a secure channel. S receives the registration (ID_i, C) from U_i and selects a 1024-bit number mk as its secret master key, which is known to this server only, also S selects a 128 bit random number r . S saves some parameters into smart card and sends it to user via secure channel. S also saves these parameters in its database as well. As user receives smart card SC from server S , it saves some parameters in smart Card. To access services from server S , user must login to the system. Here login phase starts.

User inputs his ID, Password and biometric at the sensor. Using reproduction procedure, smart card computes and confirms with the stored credentials. If mismatch is found, the login request is terminated immediately. Otherwise Smart Card computes ID and masked password. SC generates a random number RN_u , time stamp of user and now sends login request to S via a public channel. Now the authentication phase starts. When S receives login request from U_i , both mutually authenticate each other. After this both U_i and S establish a common shared secret key which is used in future for secure communication between them.

S receives login request at time TS_1^* and verifies maximum transmission delay. If verification is not successful, S terminates the request immediately. Otherwise S computes if $KA' = KA$ and ensures that $ID_i' = ID_i$. S searches for the pair (ID_i, r) in its database if this pair is found, S further computes and verifies other parameters. After verification S accepts the login request and considers the U_i as the authentic user. S generates a random number

RN_s and current timestamp RS_2 . S creates SK_{su} common secret key shared with the user for the current session. Finally, S sends the authentication request to the user via secure channel.

Upon receiving message from S , smart card SC verifies the timestamp TS_2 and maximum transmission delay, U_i calculate current session key shared with S as SK_{us} which is same as SK_{su} . Using this session key U_i assumes that S is an authenticate server. Also, the current session key $SK_{us} = SK_{su}$ is mutually verified and established. Figure 2.8 shows the timing diagram of first benchmark.

2.8.2 2PAKEP Security Scheme

Several protocols have been suggested and developed by researchers for mutual authentication. The benchmark selected is one of the key protocols recently proposed in the 2019 for D2D authentication and key agreement (Xu et al., 2019). The proposed scheme introduces a secure lightweight mutual authentication scheme using asymmetric encryption. In this proposed algorithm, Multi-factor authentication parameters which includes (Biometrics, Nonce, Timestamp) $OTP = BIOMETRICS \ \& \ NONCE(R)$ are used which ensures better security and help mitigating replay attacks. Despite these strengths, the proposed scheme has also some threats and weaknesses. In the proposed scheme, ID is sent as plain text without encryption on open channel, this can result in location -identity reveal attack as explained by (Loreti et al., 2018; Airehrour et al., 2018). Data is shared un-encrypted on open channel which can cause modification of timestamp resulting in replay attack. Also, this can lead to Man- in- the -Middle attack as described by (Diallo et al., 2017; Spiekermann et al., 2015; Chen & Zhao 2012).

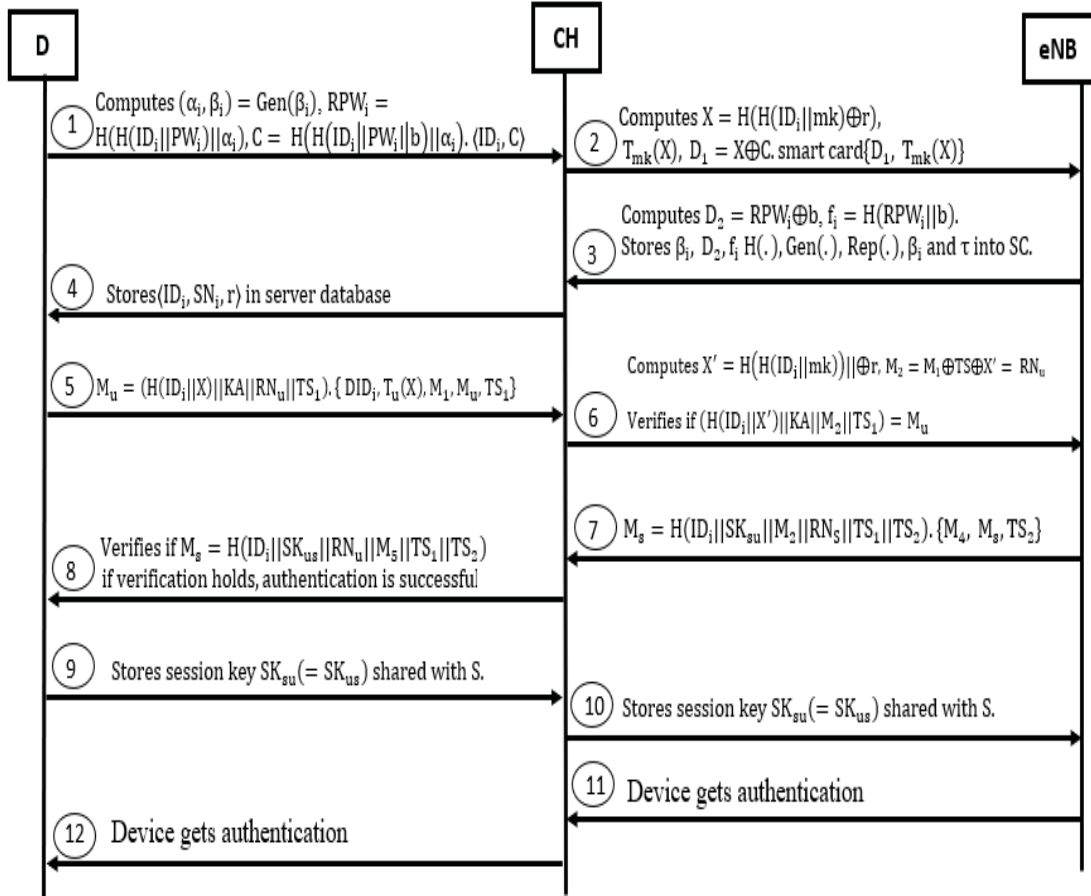


Figure 2.8: Chaotic Timing Diagram

Non-encrypted data is received at Cluster Head. This can result in Rouge relay attack by Nenvani and Gupta (2016), Yim (2016). An attacker duplicates a legitimate node in rogue relay attack which may lead to disturbance in service. The proposed scheme uses Single Hash function when sending data on open channel, this can result in Weak-collision attack by (Nimela et al., 2019; Kishore & Kappor, 2016; Mendel et al., 2009).

The proposed scheme uses some assumptions. The server is assumed to be secure and trusted node. The adversary can obtain exchanged data, modify it and replay data. It is assumed that Server Node is not physically protected. An adversary can steal information from its memory. Using the well-known Dolev-Yao threat model, it is assumed that the two

parties communicate in an insecure channel. This scheme has three phases: the initialization phase, the registration phase, and the authentication phase. The initialization phase and the registration phase are executed by the System Administrator (SA) in a secure environment. In the authentication phase, the Server Node (SN) exchanges information with the server on insecure channel and performs authentication and key agreement scheme.

First, SA generates a master key K_{ser} for the server and stores it in server memory. Then SA starts process for registering SNs and APs. For each SN, the server generates a unique identity ID_{SN} , a unique r and a random P_{Ks} . The SA stores tuple (ID_{SN}, ASN, BSN, PKs) in the SN's memory, and stores ASN , X and PKs as a tuple $\langle ASN, X, PKs \rangle$ in the server's memory. The server may store multiple such tuples. For each AP and the server generates a unique identity ID_{AP} and stores in server's memory. In authentication phase, SN generates random number $n1$ and timestamp $t1$. SN Computes and sends message $(ASN; S1; S2; t1)$ to the AP. The AP forwards this message to the server by placing its ID_{AP} . The server checks ID_{AP} and A_{SN} in its database if check fails terminates the session. Also checks the maximum transmission delay. The server also Generates $n2$, timestamp $t2$, and a unique $r+$ and Sends message $(S3; S4; S5; S6; t2; IDAP)$ to the AP. The AP forwards the information received by the server to the SN and drops its identity $IDAP$. SN checks the validity of $t2$, computes random number $n2$ and checks if Checks $S6*? = S6$. Computes Ks and replaces the parameters $A_{SN}; B_{SN}; P_{Ks}$ with the parameters $A^+_{SN}; B^+_{SN}; P^+_{Ks}$ respectively in its memory. Store session key Ks . Figure 2.9 shows the timing diagram of two-factor timing diagram.

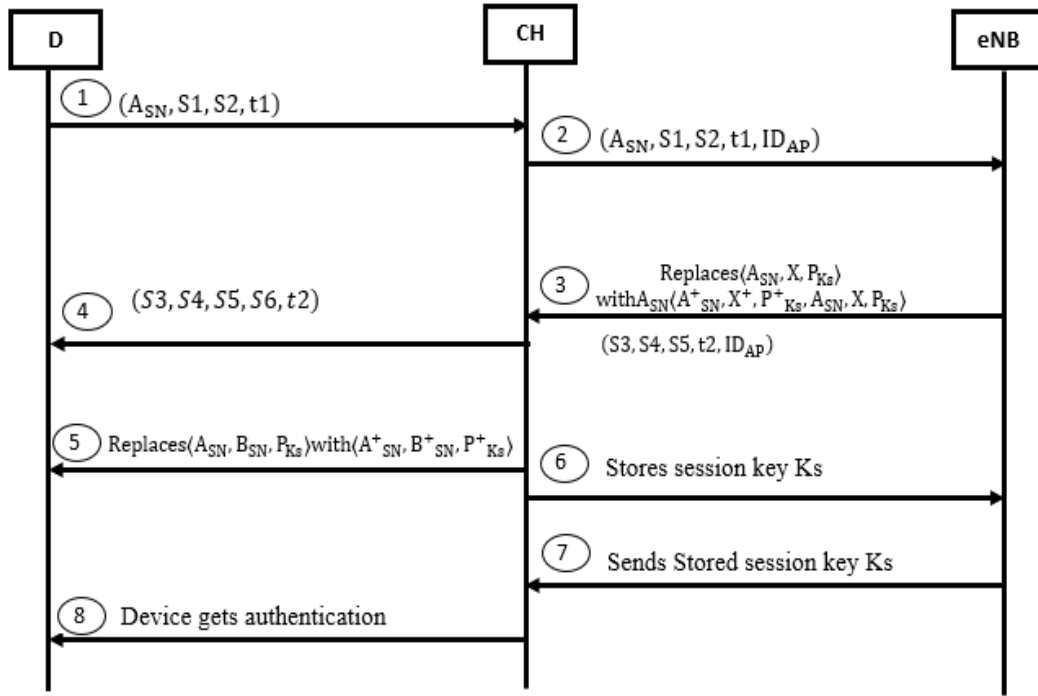


Figure 2.9: 2PAKEP Timing Diagram

2.8.3 Two Factor Security Scheme

This is another benchmark in which mutual authentication scheme is proposed by Park et al. (2018). It is based on multi factors like password, random number and smart card. The proposed scheme uses some assumptions that all devices are synchronized, and the open channel is secure. This scheme helps in mitigating replay attack and provides Multi-level Hashing for rigorous authentication and integrity. The proposed scheme also provides Quantum attack safety.

Despite above strengths of the proposed scheme in this paper, the proposed algorithm is still vulnerable to some threats and weaknesses. In the proposed scheme, ID is sent as plain text without encryption on open channel, this can result in location -identity reveal attack as explained by Loreti and Airehrour (2018). When data is sent from user to Cluster

Head, an unencrypted message is sent on open channel which can cause modification of message and hence can result in Man in the Middle attack (MITM) by Nenvani and Gupta (2016). Hash of data is sent without timestamp; this can cause Replay Attack Melki et al. (2019). Smart card is used as multi factor authentication. Smart card is vulnerable to Identity theft & Duplication of card threats by Amin et al. (2017) while also extra card reader is required.

In this scheme, the first phase is registration phase. The user U_i chooses ID_i , Password PW_i and random number r_i . The user computes pseudo PID_i and Hash HID_i and send to Server S on secure channel. The Server S randomly chooses a number n_i as it receives PID_i and Hash HID_i . The server S sends a smart card SC with parameters AID_i , $\sim n$, and PWN_i to the user U_i . The random number r_i is stored when the user U_i receives the smart card SC . Finally, the secret parameters AID_i , $\sim n$, PWN_i and r_i are stored on the smart card. Now the login phase starts. The user U_i inserts his smart card SC into the card reader and inputs ID_i and computes HID_i and send this to server S . Server generates a random number k_i . Server sends k_i and SKD_i to user. The card reader computes SK_i and send HID'_i to the smart card. The smart card SC checks $HID_i = HID'_i$. If the condition is true the user U_i can put his password PW_i , otherwise the session is terminated. The smart card checks if $PWN'_i = PWN_i$. If condition is true, then user moves to next step otherwise the session is terminated. The smart card SC chooses a random number a_i and computes A_i . Then A_i , CID_i , MID_i , and Tu_1 are sent to the server S . Figure 2.10 shows a timing diagram of 2PAKEP.

Once verification phase starts. After receiving A_i , CID_i , MID_i , and Tu_1 , the server check time stamp maximum transmission delay. If $Ts_1 = Tu_1$, it means condition is true otherwise session is terminated. The server performs further steps. The server computes and

verifies if $HID_i = HID'_i$, also checks $MID_i = MID'_i$, if the equality holds, then the server moves to next step. The server chooses random number b_i and computes B_i . Then, B_i , VID_i and T_{s2} are sent to user U_i at time T_{s2} . The user U_i receives the above information at time T_{u2} . U_i checks $T_{u2} = T_{s2}$ and $VID'_i = VID_i$. If it is true, then proceed to further step. The User U_i sends WID_i and T_{u2} to the server. When the server receives this information, it checks maximum transmission delay $T_{s3} = T_{u2}$. When conditions hold, S computes and checks $WID_i = H_1(VID_i = H_1(VID_i) || LB_{ix} || LB_{iy} || T_{u2})$. When the equality in this judgment equation holds, the authentication succeeds. Otherwise, the authentication fails, and the session is terminated.

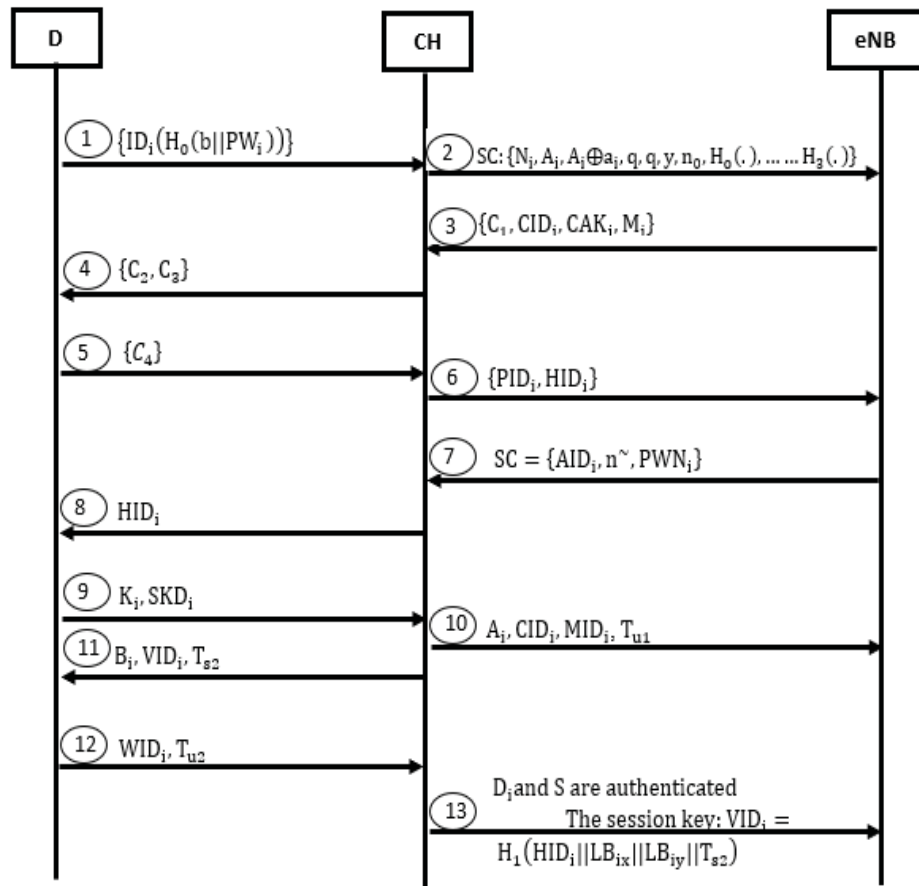


Figure 2.10: TwoFactor Timing Diagram

Table 2.2 defines the various attacks that have been mitigated by each benchmark protocol and the proposed protocol.

Table 2.2: Attacks Mitigated by Protocols

Attack Type	LEMAP	2PAKEP	TwoFactor	Chaotic
A Preimage attack	Yes	No	No	No
Man in The Middle Attack (MITM)	Yes	Yes	Yes	Yes
Impersonation Attacks	Yes	Yes	Yes	Yes
Privileged-Insider Attack	Yes	Yes	Yes	No
Mutual Authentication	Yes	Yes	Yes	Yes
Replay Attack	Yes	Yes	Yes	Yes
Password Change attack	No	Yes	Yes	Yes
Pass-the-Hash (PtH) attack	Yes	No	No	No
Masquerading Attack	Yes	No	No	No
Repudiation Attack	Yes	No	No	No
Denial of Service Attack.	Yes	No	No	No
Eavesdropping attack	Yes	No	No	Yes
Rogue Relay Attack	Yes	No	No	No
Malicious Card Reader Attack	No	No	Yes	Yes

2.9 Analysis Method

BAN logic proof was proposed by Burrows and Abadi in 1989. Authentication protocols are the basis of security in many systems. In order to ensure the correctness of a proposed scheme, many studies offer the BAN logic model to prove that their authentication protocols are effective, using many logic symbols and formula rules in the proof process.

The proposed scheme LEMAP has been verified and analyzed using BAN Logic in Chapter 4. The correctness of the proposed scheme is verified against different security threats and attacks. Benchmark protocols have also been analyzed using BAN Logic and compared with the proposed scheme. Compared with previous schemes, the main advantages of the proposed scheme are its low computation and communication cost, guaranteed security and better adaptability to actual client server communication environments.

2.10 Summary

In this Chapter, an overview of D2D communication, different modes of D2D communication, components of D2D and D2D security protocols have been discussed. The related work and research done so far in D2D security has also been discussed. The chapter also describes about security requirements for D2D communication and threats involved in D2D security. Detailed explanation is presented about security challenges and attacks in D2D. Security threats and proposed schemes in benchmarks have been explained. Threats mitigated by different benchmark protocols and the proposed scheme LEMAP is presented to show how much better security proposed algorithm offers. Benchmark algorithm and the proposed scheme all use ECC for lightweight and strong encryption. This chapter discusses the major security issues which can be faced and encountered using security algorithms and security requirements that any security algorithms should meet. Finally, this chapter

discusses the performance analysis method BAN Logic used in literature to validate and verify the correctness of the proposed security schemes.

CHAPTER 3

SYSTEM DESIGN FOR LEMAP SCHEME

3.1 Introduction

Device to Device (D2D) communication is a peer-to-peer communication mechanism between devices without need to communicate through intermediate node and operates in a highly open and dynamic environment. Despite many advantages of D2D multi-hop communication, there are many security challenges associated with D2D and it is vulnerable to several security threats. To securely operate D2D and to overcome challenges it faces, a multi-factor authentication security mechanism is required. This chapter aims to introduce a Lightweight ECC based Multi-Factor Authentication Protocol (LEMAP) for Device to Device Multi-hop Cellular Communication. The first section of the chapter discusses details of multi-factors which work combine to provide secure and lightweight security algorithm for secure D2D communication. Once mutual authentication is done using multi-factors and device trust is validated then devices can communicate securely over open channel. D2D communication allows devices to act as a non-transparent relay (NTR) where participating devices can decode and forward requests to the neighboring devices. Formal methods provide validation of proposed security mechanism. BAN logic has been used to analyze the secrecy of LEMAP and other benchmarking security schemes. D2D requires security schemes to be lightweight and computationally inexpensive. Computation and authentication cost have been analyzed to ensure minimal overhead for the proposed scheme. Introduction of computationally powerful computers has made most of the security schemes vulnerable to baseline attacks such as brute force or intelligent attacks. Pollard rho (Montenegro & Tetali, 2005) and Baby step Giant step (BsGs) methods are used to check

proposed scheme against quantum attacks. Security scheme is proven to be safe against any security attacks based on high power computational machines using Discrete Logarithm Problem (DLP).

3.2 System Model

To secure multi-hop D2D communication, Multi-Factor Authentication (MFA) layer and Security layer are introduced as sublayers to the main security layer. Block diagram of both layers is shown in Figure 3.1.

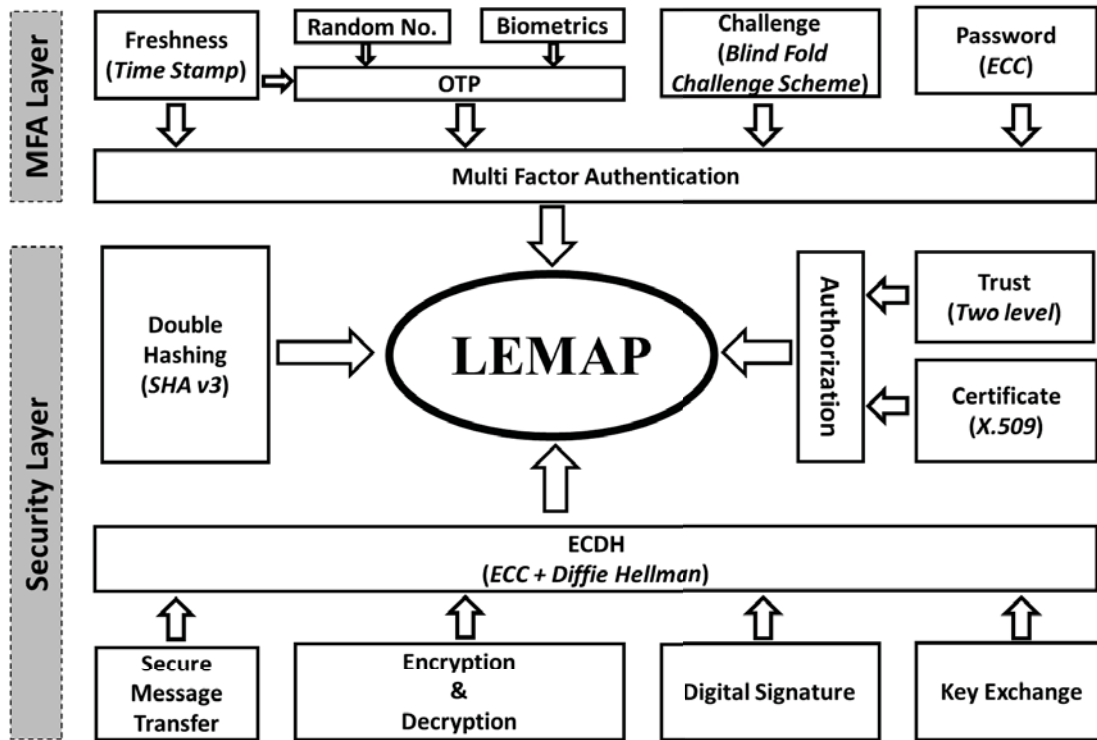


Figure 3.1: System Model of LEMAP

3.2.1 Multi Factor Authentication Layer

Multi Factor Authentication layer consists of five components timestamp, random number, biometric, challenge, and password. Pseudo IDs are assigned to devices to hide real

identity during communication so that adversary should not be able to know actual identity and location of the participating device. This helps to secure communication from identity reveal attack. Onetime password OTP is generated using random number with specific time validity. Each device must respond and solve OTP to get validity trust from eNB to communicate with other devices. If device is unable to respond OTP within the specific time period, its validity expires which secures communication from malicious attackers, who may try to use OTP after some time. Each request message is sent along with a challenge and every response is required to solve this challenge.

When a message is sent, its hashed challenge solution is also sent with the actual message. When a receiver receives the message and solves the challenge, it decrypts the already sent solved challenge and compares it with the solution. If solved challenge and sent challenge solution are same, the message is considered valid and trusted. Blind Fold Challenge Scheme is used in this algorithm to create challenge and challenge solution. Timestamp is another factor used to check the message freshness and verify it for replay attack. If the message is responded within the timestamp, the message is considered fresh and free of any replay attack. All these above-mentioned factors combine to develop LEMAP a multi-factor authentication protocol to secure D2D communication with less authentication overhead and lightweight in communication and computation cost.

3.2.2 Security Layer

Security layer comprises four major components which include secure message transfer, encryption & decryption, digital signature and key exchange. Key creation module is responsible for the creation of a secret point for communication. For this purpose, Elliptic Curve Cryptography (ECC) based algorithm is used. Secure Key transmission is very

important part of secure D2D communication where secret keys generated using ECC are securely transmitted. Elgamal algorithm is used for sharing key and sending encrypted messages. For message freshness, timestamp is used and this will secure the message from replay attack. To secure messages from MITM attack, a simple Challenge-Response authentication scheme is used. This scheme will also ensure the delivery of the message. To ensure integrity of the message, double hashing technique is used which helps to avoid collisions in hash tables. The reason for collision is when two keys are hashed to the same index in a hash table. The double hashing is done using SHA v3 algorithm. In cryptographic module, encryption and decryption of data is done which is received at any device or eNB. ECC is used for both encryption and decryption, which is lightweight and has small key size.

3.2.3 LEMAP for D2D Multi-hop Communication

The following section explains the Lightweight ECC based Multi-Factor Authentication Protocol (LEMAP) for Device to Device Multi-hop Communication security scheme and its components in detail as well as the procedure to achieve mutual authentication and security.

3.2.4 Notations Table for LEMAP (NTL)

Table 3.1 describes complete set of notations with their symbols and description, used in LEMAP. D_1 , D_2 represent two devices which want to communicate with each other. CH represents Cluster Head that works as relay agent to forward request and response messages to other devices. eNB is a Base Station with strong coverage and ability to provide authentication and authorizations to devices in its area. Challenge is denoted by Ch which is used in each message to give challenge to other device. DH represents double hash which is used in each request and response message. Onetime password is denoted by OTP used by

devices to verify its validation and to get authorization. PID is used for Pseudo Identity to hide real identity of devices during communication. P represents public key that is used in LEMAP communication to encrypt messages with public key of the receiver. Pr denotes private key to digitally sign the message sent to other devices.

Table 3.1: Notations Table for LEMAP

Name	Symbol	Description
D ₁	Device 1	Device 1 participating in D2D communication
D ₂	Device 2	Device 2 participating in D2D communication
CH	Cluster Head	Forwarding or relay device
eNB	Evolved node Base Station	Base Station with strong coverage and authorizations
Challenges	Ch _{CH}	Challenge of Cluster Head
	Ch _{CH} '	Challenge Solution of Cluster Head
	Ch _{D₁}	Challenge of device1
	Ch _{D₁} '	Challenge Solution of device1
	Ch _{D₂}	Challenge of Device2
	Ch _{D₂} '	Challenge solution of Device2
	Ch _{eNB}	Challenge of device1
	Ch _{eNB} '	Challenge Solution of eNB

Table 3.1 continued

Double Hash	DH	Double Hash
One Time Password	OTP_{CH}	Onetime Password of Cluster Head
	OTP'_{CH}	Onetime Password Solution of Cluster Head
	OTP_{D1}	Onetime password of device 1
	OTP'_{D1}	Onetime password solution of device1
	OTP_{D2}	Onetime password of device 2
	OTP'_{D2}	Onetime password solution of device 2
	OTP_{eNB}	Onetime Password of eNB
Pseudo Identities	PID_1	Pseudo ID of device1
	PID_2	Pseudo ID of device2
Public Keys	P_{D1}	Public key of device1
	P_{D2}	Public key of device2
	P_{CH}	Public key of Cluster Head
Private Keys	Pr_{CH}	Private key of Cluster Head
	Pr_{D1}	Private key of device 1
	Pr_{D2}	Private key of device 2
	Pr_{eNB}	Private key of eNB

Table 3.1 continued

Timestamp	T_{SCH}	Timestamp of Cluster Head
	T_{SeNB}	Timestamp of eNB
	T_{SD_1}	Timestamp of device1
	T_{SD_2}	Timestamp of Device2
Validation of Device	VD_1 ,	Validating of device1
	VD_2	Validating of device2

3.2.5 Factors Attacks Mitigation Table for LEMAP (FMT)

Table 3.2 also called Factors Attack Mitigation Table for LEMAP (FMT) which explains different notations used in LEMAP with purpose and attacks mitigated by each factor. **Ch** Challenge is used for achieving mutual authentication which helps mitigating MITM attack allowing only legitimate cellular devices. **PID** is used to keep privacy and helps in mitigating Location Based Identity attack. **T_s** timestamp is used to check message freshness and helps to mitigate replay attack. **DH** Double Hashing is used to achieve integrity and helps to mitigate preimage and MITM attack. **P_r** Private key is used to achieve confidentiality and helps in mitigating impersonation attack. **OTP** Onetime password ensures device legitimacy and helps in mitigation of time-stamp exploitation attack. **P** Public key is used to encrypt data to secure data from masquerading attack. **VD₁** and **VD₂** Validate the devices to provide services to legitimate device only and help mitigation of rouge device attack.

Table 3.2: Factors Attacks Mitigation Table for LEMAP (FMT)

Notation	Purpose	Attack Mitigation
Ch	Challenge is used for mutual authentication	Mitigating malware attack allowing only legitimate cellular devices
PID	Pseudo ID is kept for achieving anonymity and privacy	Mitigating Location Based Identity attack
T _s	Time stamping is used for achieving freshness	Mitigating replay attack
Ch'	Challenge Solution is sent in order to ensure receiver is a genuine cellular device	Mutual Authentication
DH	Double Hashing is done to achieve • Integrity of message • Confusion and diffusion	Mitigating Pre-image attack or weak Collision attacks, MITM attack and modification data attack
P _r	Private key is used to digitally sign data and achieve confidentiality	Mitigating impersonation and MITM attack

Table 3.2 continued

OTP	One-time password ensures authentication, Renewal of registration, Biometrics. (Legitimacy of cellular device)	Mitigation of time-stamp exploitation attack, timing-window attack using replay attack and Whitewash attack
P	Public key is used to encrypt data	Issuing public key will ensure Mitigation of Masquerading attack
VD ₁	Validate the device and provide services to legitimate device. Also provide authorization and validation at two levels	Mitigation of rouge device attack.
VD ₂	Validate the device and provide services to legitimate device. Also provide authorization and validation at two levels	Mitigation of rouge device attack.

3.3 System Design for LEMAP

This protocol used ECC for encryption and decryption due to its small key size and lightweight while Elgamal is used for key exchange. This protocol has been developed by using multi factors like onetime password, random number, challenge and timestamp to get secure mutual authentication. ECC with Elgamal helps to reduce authentication overhead, communication cost and low computation cost. Hence LEMAP protocol ensures asymmetric

cryptography, authentication, integrity, confidentiality and quantum attack safety. The proposed algorithm LEMAP steps are explained in detail below:

3.3.1 Authentication Request Message (D1- CH)

Equation 3.1 is an Authentication Request Message (D1- CH) for communication between D₁ and D₂. The security threat associated with this message and how message is encrypted and decrypted is explained as below:

$$\left\{ \begin{array}{l} \left\{ \text{PID}_1, \text{PID}_2, \text{PICH}, \text{PIeNB}, \text{Ch}_{D_1-\text{CH}}, \text{T}_{S_{D_1}}, \left[\text{DH} \left(\text{PID}_1, \text{PID}_2, \text{PICH}, \text{PIeNB}, \text{Ch}_{D_1-\text{CH}}', \text{T}_{S_{D_1}} \right) \right]_{P_{rD_1}} \right\}_{P_{CH}} \\ \left\{ \text{PID}_1, \text{PID}_2, \text{Ch}_{D_1-\text{eNB}}, \text{T}_{S_{D_1}}, \left[\text{DH} \left(\text{PID}_1, \text{PID}_2, \text{Ch}_{D_1-\text{eNB}}', \text{T}_{S_{D_1}} \right) \right]_{P_{rD_1}} \right\}_{P_{eNB}} \end{array} \right\}_{P_{CH}} \quad \text{Equation 3.1}$$

3.3.1.1 Potential Security Threats

The Authentication Request Message in Equation 3.1 is vulnerable to the attacks such as rouge devices attack where a fake device can claim to be CH. The messages can be used to do preimage attack on other devices by getting a message forwarded from legitimate CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.1.2 Encryption Mechanism

To counter above mentioned attacks, the request message in Equation 3.1 is prepared by using three credentials i.e. pseudo ID for devices D₁ and D₂, CH and eNB, challenge and timestamp. This message also contains double hash value of pseudo ID, solution of challenge and timestamp which is signed by the private key P_{rD₁} of D₁. The message is signed by public key of CH. The second portion of the message contains authentication request for eNB

containing credentials pseudo ID, challenge for eNB and timestamp. The message contains double hash value of the pseudo ID, solution of challenge and timestamp which is signed by the private key of device D_1 and encrypted with public key of eNB. Later, the whole Auth-Req (D_1 -CH) is encrypted by the public key of CH.

As discussed in Table 3.2, usage of pseudo ID, challenge and timestamps can mitigate identity reveal attack, malware attack, timestamps exploitation attack, replay attack, denial of service attack, man in the middle attack and data modification attack. While double hashing the solution of challenge, one-time password and timestamp can ensure integrity of the data which means no data is modified during the entire communication. This also mitigates weak collision attack, man in the middle attack and pre-image attack. The message also includes challenge solution during double hashing process. The purpose of sending challenge is to ensure receiver is a genuine cellular device which means it is not bot. It also minimizes the chances of denial of service attack and rogue device attack. The double hash value is encrypted by private key of the sender (eNB) to ensure the message is sent by the legitimate device thus mitigating the rogue device attack, impersonation attack. Finally, the entire message is encrypted by public key of the receiver to maintain the secrecy of the message.

3.3.1.3 Decryption Mechanism

Once CH receives the authentication request message in Equation 3.1 from D_1 , it will use its own private key to decrypt the entire message. Once the message is decrypted, it will check given challenge, pseudo ID and timestamp. CH will address the challenge and check either the timestamp is fresh or not. Later, CH will decrypt double hash value of challenge solution, pseudo ID and timestamp. CH will utilize its own public key to decrypt the double hash value sent by D_1 in encrypted version. Later, CH will match both values encrypted and

sent by D_1 and double hashed values generated by CH, if both values are same it means the data integrity is maintained.

3.3.2 Authentication Request Message (CH- eNB)

Equation 3.2 is an Authentication Request Message (CH- eNB) from CH to eNB. CH forwards the request message from D_1 to eNB. The security threat associated with this message and how message is encrypted and decrypted is explained as below:

$$\left\{ \left\{ \begin{array}{l} PID_1, PID_2, Ch_{D_1-eNB}, T_{S_{D_1}}, \\ [DH(PID_1, PID_2, Ch_{D_1-eNB}', T_{S_{D_1}})]_{Pr_{D_1}} \end{array} \right\}_{PeNB}, \right. \quad \text{Equation 3.2} \\ \left. \left\{ \begin{array}{l} PID_1, PID_2, PICH, Ch_{CH-eNB}, T_{S_{CH}}, \\ [DH(PID_1, PID_2, PICH, Ch_{CH-eNB}', T_{S_{CH}})]_{Pr_{CH}} \end{array} \right\}_{PeNB} \right\}$$

3.3.2.1 Potential Security Threats

The Authentication Request Message (CH-eNB) in Equation 3.2 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. The attack such as Identity reveal attack is also possible in case of CH being compromised. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.2.2 Encryption Mechanism

To counter already discussed attacks, the request message in Equation 3.2 is prepared by using three credentials i.e. challenge, pseudo ID of devices D_1 , D_2 and timestamp. This message also contains double hash value of pseudo IDs, challenge solution and timestamp which is signed by the private key of device D_1 and encrypted with public key of eNB. The message second portion contains request message for eNB containing credentials pseudo IDs, challenge and timestamp. This message also contains double hash value of the pseudo

IDs, challenge solution and timestamp which is signed by the private key of CH. The whole message Auth-Req (CH-eNB) is encrypted with public key of eNB.

As discussed in Table 3.2, usage of pseudo ID, challenge, and timestamp can mitigate identity reveal attack, timestamp exploitation attack, replay attack, pre-image attack, man in the middle attack, rogue device attack, weak collision attack and data modification attack. While double hashing pseudo IDs, challenge solution and timestamp mitigate weak collision attack, replay attack, man in the middle attack and pre-image attack. The message also contains challenge solution during double hashing process. The purpose of sending challenge is to ensure the receiver is a genuine cellular device and it is not bot. This mitigates denial of service attack and rogue device attack. The double hashed value is encrypted by private key of the sender (CH) to ensure the message is sent by the legitimate device thus mitigating the impersonation attack. Finally, the entire message is encrypted by public key of the receiver to maintain secrecy of the message and mitigating masquerading attack.

3.3.2.3 Decryption Mechanism

Once CH receives the authentication request message in Equation 3.2 from D_1 , it will use its own private key to decrypt the entire message. When the message is decrypted, it will check challenge given, pseudo ID and timestamp. CH will address the challenge and check either the timestamp is fresh or not. Later, CH will find double hash value of pseudo ID, challenge solution and timestamp. eNB will utilize its own public key to decrypt the double hash value sent by CH in encrypted version. Later, eNB will match both double hash value i.e generated by eNB and the value sent by CH, if both values match, it means the data integrity is maintained.

3.3.3 Authentication Response Message (eNB- CH)

Equation 3.3 is an Authentication Response Message (eNB- CH) from eNB to CH. CH gets OTP request message from eNB. The security threat associated with this message and how it is encrypted and decrypted is explained as below.

$$\left\{ Ch_{eNB-CH}, T_{SeNB}, OTP_{eNB-CH}, [DH(Ch_{eNB-CH}', T_{SeNB}, OTP_{eNB-CH}')]_{Pr_{eNB}} \right\}_{P_{CH}} \quad \text{Equation 3.3}$$

3.3.3.1 Potential Security Threats

Authentication Response Message (eNB- CH) Equation 3.3 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.3.2 Encryption Mechanism

To counter above mentioned attacks, the response message Equation 3.3 is prepared by utilizing three credentials i.e. challenge, timestamp and one-time password. This message also contains double hash value of the challenge solution, one-time password and timestamp which is signed by the private key of eNB. Later the Auth-Res (eNB-CH) is encrypted by the public key of CH. As discussed in Table 3.2, usage of challenge, one-time password and timestamps can mitigate timestamps exploitation attack, replay attack, rogue device attack and man in the middle attack. While double hashing the challenge solution, one-time password and timestamp can ensure integrity of data which means there is no data modification during the entire communication. The double hash value is encrypted by private key of the sender (eNB) to ensure the message is sent by the legitimate user thus mitigating

the impersonation attack. The entire message is encrypted by public key of the receiver to maintain secrecy of the message.

3.3.3.3 Decryption Mechanism

Once CH receives the authentication response message from eNB, CH will use its own private key to decrypt the entire message. When the message is decrypted, it will check challenge given by eNB, OTP and timestamp. CH will solve the challenge, use OTP and check the timestamp freshness. Later, CH will utilize public key of eNB to decrypt the double hash values of challenge solution, one-time password and timestamp sent by eNB. If double hash values generated by CH and the other sent by eNB match, it means data integrity is maintained.

3.3.4 Authentication Request Message (CH- eNB)

Equation 3.4 is an Authentication Request Message (CH- eNB) from CH to eNB. CH solves OTP and sends request message to eNB for authentication. The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left\{ \begin{array}{l} Ch_{CH-eNB}, T_{SCH}, OTP'_{CH-eNB}, \\ [DH(Ch'_{CH-eNB}, T_{SCH}, OTP'_{CH-eNB})]_{Pr_{CH}} \end{array} \right\}_{PeNB} \quad \text{Equation 3.4}$$

3.3.4.1 Potential Security Threats

The Authentication Request Message (CH-eNB) Equation 3.4 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.4.2 Encryption Mechanism

To counter above mentioned attacks, the request message Equation 3.4 is prepared by utilizing three credentials i.e. challenge, timestamp and onetime password solution. This message also contains double hash value of the challenge solution, timestamp and onetime password solution which is signed by the private key of CH. The whole Auth-Req (CH-eNB) message is encrypted with public key of eNB. Onetime password solution is sent by CH to eNB to verify that if CH is a valid and legitimate device. While double hashing of onetime password solution, challenge solution and timestamp signed by private key of CH can ensure integrity of data which means data is not modified during transmission. This can also mitigate rouge device attack, replay attack, man in the middle attack, impersonation attack and pre-image attack. The double hash value is encrypted by private key of the sender (CH) to ensure the message is sent by the legitimate device hence mitigating impersonation attack. The entire message is encrypted by public key of the receiver eNB to maintain the secrecy of the message which mitigates masquerading attack.

3.3.4.3 Decryption Mechanism

Once eNB receives the authentication request message from CH, it will use its own private key to decrypt the entire message. When the message is decrypted, it will check onetime password solution, challenge given and timestamp freshness. eNB will utilize public key of CH to decrypt encrypted message sent by CH. Then eNB will match both double hash values i.e. generated by eNB and other sent by CH, if both values match it means data integrity is maintained.

3.3.5 Authentication Response Message

Equation 3.5 is an Authentication Response Message from eNB to CH. eNB sends OTP to D₁ and D₂. The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left(\begin{array}{l} \text{PICH} | \text{P}_{\text{CH}}, \text{PID}_1 | \text{P}_{\text{D}_1}, \text{PID}_2 | \text{P}_{\text{D}_2} |, \\ \text{Ch}_{\text{eNB-CH}}, \text{T}_{\text{SeNB}}, [\text{DH}(\text{Ch}_{\text{eNB-CH}'}, \text{T}_{\text{SeNB}})]_{\text{P}_{\text{reNB}}}, \\ \left\{ \begin{array}{l} \text{Ch}_{\text{eNB-D}_1}, \text{T}_{\text{SeNB}}, \text{OTP}_{\text{eNB-D}_1} \\ , [\text{DH}(\text{Ch}_{\text{eNB-D}_1'}, \text{T}_{\text{SeNB}}, \text{OTP}_{\text{eNB-D}_1'})]_{\text{P}_{\text{reNB}}} \end{array} \right\}_{\text{P}_{\text{D}_1}} \\ , \left\{ \begin{array}{l} \text{Ch}_{\text{eNB-D}_2}, \text{T}_{\text{SeNB}}, \text{OTP}_{\text{eNB-D}_2} \\ , [\text{DH}(\text{Ch}_{\text{eNB-D}_2'}, \text{T}_{\text{SeNB}}, \text{OTP}_{\text{eNB-D}_2'})]_{\text{P}_{\text{reNB}}} \end{array} \right\}_{\text{P}_{\text{D}_2}} \end{array} \right)_{\text{P}_{\text{CH}}} \quad \text{Equation 3.5}$$

3.3.5.1 Potential Security Threats

The Authentication Response Message (eNB-CH) Equation 3.5 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.5.2 Encryption Mechanism

To counter above mentioned attack, the Authentication response message, Equation 3.5 is formed by utilizing three credentials i.e. challenge, timestamps and onetime password (OTP). This message also contains double hashed value of challenge solution and timestamp which is signed by the private key of eNB. The message also contains messages for devices D₁ and D₂ which consists of three credentials challenge, timestamp and onetime password. This messages also contain double hash value of the challenge solution, timestamp and

onetime password which is signed by the private key of eNB and encrypted with public key of devices D_1 and D_2 . The whole message is encrypted by public key of CH.

As discussed in Table 3.2, challenge, timestamp and onetime password can mitigate rogue device attack, timestamp exploitation attack, replay attack, pre-image attack, weak collision attack, man in the middle attack and data modification attack. While double hashing the challenge solution, timestamp and onetime password can ensure integrity of the data which means no data is modified during entire communication and it also mitigates rogue device attack, man in the middle attack and pre-image attack. The messages for devices D_1 and D_2 contain onetime password (OTP) for both devices to solve to verify legitimacy. The double hash value is encrypted by private key of the sender (eNB) to ensure the message is sent by the legitimate device so mitigating the impersonation attack. The entire message is encrypted by public key of the receiver to maintain secrecy of the message and hence mitigating masquerading attack.

3.3.5.3 Decryption Mechanism

Once CH receives the authentication response message from eNB, it will use its own private key to decrypt the entire message. When the message is decrypted, it will check challenge given and timestamp to verify message freshness. Then CH will match both double hashed values i.e generated by CH and other sent by eNB, if both values match it means data integrity is maintained. CH cannot open messages for D_1 and D_2 sent by eNB. CH will forward these messages to devices D_1 and D_2 .

3.3.6 Authentication Response Message

Equation 3.6 is an Authentication Response Message where CH forwards OTP to D₁. The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left\{ \begin{array}{l} \left\{ Ch_{eNB-D_1}, T_{SeNB}, OTP_{eNB-D_1} \right\} \\ \left\{ [DH(Ch'_{eNB-D_1}, T_{SeNB}, OTP_{eNB-D_1})]_{Pr_{eNB}} \right\}_{P_{D_1}} \end{array} \right\} \quad \text{Equation 3.6}$$

$$\left\{ \begin{array}{l} Ch_{CH-D_1}, T_{SCH} \\ [DH(Ch'_{CH-D_1}, T_{SCH})]_{Pr_{CH}}, PICH|P_{CH}, PID_1|P_{D_1}, PID_2|P_{D_2} \end{array} \right\}_{P_{D_1}}$$

3.3.6.1 Potential Security Threats

The Authentication Response Message, Equation 3.6 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.6.2 Encryption Mechanism

To counter above mentioned attacks, the response message, Equation 3.6 is prepared by utilizing two credentials i.e. challenge and timestamp. This message also contains double hashed value of challenge solution and timestamp which is signed by the private key of CH. The message also contains public keys of CH, D₁ and D₂. The first portion of the message is sent from eNB for D₁ which contains challenge, timestamp and onetime password (OTP). This message is encrypted with public key of D₁.

As discussed in Table 3.2, challenge and timestamp can mitigate timestamp exploitation attack, replay attack, pre-image attack, weak collision attacks, man in the middle attack and modification of data attack. While double hashing the challenge solution and

timestamp can also mitigate weak collision attack, man in the middle attack and pre-image attack. The purpose of sending challenge is to ensure receiver is a genuine cellular device. The double hash value is encrypted by private key of the sender (CH) to ensure the message is sent by the legitimate user hence mitigating the impersonation attack. Finally, the entire message is encrypted by public key P_{D1} of the receiver to maintain the secrecy of the message and, hence mitigating masquerading attack.

3.3.6.3 Decryption Mechanism

Once the D_1 receives the authentication response message from CH, it will use its own private key to decrypt the entire message. When the message is decrypted, it will check challenge given, OTP and timestamp. D_1 will address the challenge, use OTP and check either the timestamp is fresh or not. Later, D_1 will check double hash values of challenge solution, timestamp and OTP sent by eNB and match with values sent by CH. If both values match, it means the data integrity is maintained.

3.3.7 Authentication Response Message

Equation 3.7 is an Authentication Response Message, where CH forwards OTP to D_2 . The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left\{ \left\{ \begin{array}{l} Ch_{eNB-D_2}, T_{SeNB}, OTP_{eNB-D_2} \\ [DH(Ch_{eNB-D_2}, T_{SeNB}, OTP_{eNB-D_2})]_{Pr_{eNB}} \end{array} \right\}_{P_{D_2}}, \left\{ \begin{array}{l} Ch_{CH-D_2}, T_{SCH}, [DH(Ch_{CH-D_2}', T_{SCH})]_{Pr_{CH}} \\ , PICH|P_{CH}, PID_1|P_{D_1}, PID_2|P_{D_2} \end{array} \right\}_{P_{D_2}} \right\} \quad \text{Equation 3.7}$$

3.3.7.1 Potential Security Threats

The Authentication Response Message Equation 3.7 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.7.2 Encryption Mechanism

To counter above mentioned attacks, the response message Equation 3.7 is prepared by utilizing two credentials i.e. challenge and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of CH. The message also contains public keys of CH, D_1 and D_2 .

The first portion of the message is sent from eNB for D_2 which contains challenge, timestamp and onetime password (OTP). This message is encrypted with public key of D_2 . As discussed in Table 3.2, challenge and timestamp can mitigate timestamp exploitation attack, replay attack, pre-image attack, weak collision attacks, man in the middle attack and modification of data attack. While double hashing the challenge solution and timestamp can also mitigate weak collision attack, man in the middle attack and pre-image attack. The purpose of sending challenge is to ensure receiver is a genuine cellular device. The double hash value is encrypted by private key of the sender (CH) to ensure the message is sent by the legitimate user hence mitigating the impersonation attack. Finally, the entire message is encrypted by public key P_{D2} of the receiver to maintain the secrecy of the message and thus mitigating masquerading attack.

3.3.7.3 Decryption Mechanism

Once the D_2 receives the authentication response message from CH, it will use its own private key to decrypt the entire message. When the message is decrypted, it will check challenge given, OTP and timestamp. D_2 will address the challenge, use OTP and check either the timestamp is fresh or not. Later, D_2 will check double hash values of challenge solution, timestamp and OTP sent by eNB and match with values sent by CH. If both values match, it means data integrity is maintained.

3.3.8 The Authentication Request Message

Equation 3.8 is an Authentication Request Message where D_1 requests CH for authentication. The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left\{ \begin{array}{l} Ch_{D_1-CH}, T_{SD_1}, \left[DH \left(Ch_{D_1-CH}', T_{SD_1} \right) \right]_{Pr_{D_1}}, \\ Ch_{D_1-eNB}, T_{SD_1}, \left\{ \left[DH \left(Ch_{D_1-eNB}', T_{SD_1} \right) \right]_{Pr_{D_1}} \right\}_{PeNB} \end{array} \right\}_{PeNB} \quad \text{Equation 3.8}$$

3.3.8.1 Potential Security Threats

The Authentication Response Message, Equation 3.8 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.8.2 Encryption Mechanism

To counter above mentioned attacks, the request message Equation 3.8 is prepared by utilizing two credentials i.e. challenge and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of D_1 .

The message also contains request message for eNB containing credentials challenge for eNB and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of device1 D_1 . Later the Auth-Req (D_1 -CH) is signed by the public key of eNB.

As discussed in Table 3.2, usage of challenge and timestamp can mitigate timestamps exploitation attack, replay attack, man in the middle attack and modification of data attack. While double hashing the challenge solution and timestamp signed by private key of the sender D_1 can ensure integrity of the data which means no data is modified during the entire communication. This also mitigates weak collision attack, man in the middle attack and pre-image attack. The message also used solution of challenge during double hashing process. The purpose of sending challenge is to ensure receiver is a genuine cellular device which means it's not bot thus also minimizing the chances of denial of service attack. The double hash value is encrypted by private key of the sender D_1 to ensure the message is sent by the legitimate user thus mitigating the impersonation attack and lastly, the entire message is encrypted by public key of the receiver to maintain secrecy of the message.

3.3.8.3 Decryption Mechanism

Once CH receives the authentication request message from D_1 , it will use its own private key to decrypt the entire message. Once the message is decrypted, it will check challenge given and timestamp. CH will address the challenge and check either the timestamp is fresh or not. Later, CH will check double hash values of challenge solution and timestamp. CH will utilize its own public key to decrypt the double hash value sent by D_1 in encrypted version. Later, CH matches both values, if double hashed values i.e. generated by CH and other sent by D_1 match, it means the data integrity is maintained.

3.3.9 Auth-Request Message

Equation 3.9 is an Authentication Request Message where D2 requests CH for authentication. The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left\{ \begin{array}{l} \text{Ch}_{D_2-CH}, T_{SD_2}, \left[\text{DH} \left(\text{Ch}_{D_2-CH}', T_{SD_2} \right) \right]_{Pr_{D_2}}, \\ \text{Ch}_{D_2-eNB}, T_{SD_2}, \left\{ \left[\text{DH} \left(\text{Ch}_{D_1-eNB}', T_{SD_1} \right) \right]_{Pr_{D_1}} \right\}_{PeNB} \end{array} \right\}_{PeNB} \quad \text{Equation 3.9}$$

3.3.9.1 Potential Security Threats

The Authentication Response Message, Equation 3.9 is vulnerable to is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.9.2 Encryption Mechanism

To counter above mentioned attacks, the request message is prepared by utilizing two credentials i.e. challenge and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of D₂. The message also contains request message for eNB with credentials challenge and timestamp. The message also contains double hash value of challenge solution and timestamp which is signed by the private key of device D₂. Later the Auth-Req is signed by the public key of eNB.

As discussed in Table 3.2, usage of challenge and timestamp can mitigate timestamps exploitation attack, replay attack and man in the middle attack. While double hashing the challenge solution and timestamp signed by private key of the sender D₂ can ensure integrity

of the data which means no data is modified during the entire communication, hence mitigating data modification attack. The message also used solution of challenge during double hashing process. The purpose of sending challenge is to ensure receiver is a genuine cellular device which also minimizes the chances of denial of service attack. The double hash value is encrypted by the private key of the sender (D_2) to ensure the message is sent by the legitimate user so mitigating the impersonation attack. The entire message is encrypted by public key of the receiver to maintain the secrecy of the message.

3.3.9.3 Decryption Mechanism

Once CH receives the authentication request message from D_2 , it will use its own private key to decrypt the entire message. When the message is decrypted, it will check challenge given and timestamp. CH will address the challenge and check either the timestamp is fresh or not. Later, CH will check double hash values of challenge solution and timestamp. CH will use its own public key to decrypt the double hash value sent by D_2 in encrypted version. Later, CH will match both values, if double hash values i.e generated by CH and other sent by D_2 match, it means the data integrity is maintained.

3.3.10 Authentication Request Message

Equation 3.10 is an Authentication Request Message where CH forwards requests from $D1$ and $D2$ to eNB to validate both devices. The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left(\begin{array}{l} Ch_{D_1-eNB}, T_{SD_1}, \left\{ \left[DH \left(Ch_{D_1-eNB}', T_{SD_1} \right) \right]_{Pr_{D_1}} \right\}_{PeNB}, \\ Ch_{CH-eNB}, T_{SCH}, \left[DH \left(Ch_{CH-eNB}', T_{SCH} \right), VD_1 \right]_{Pr_{CH}} \\ Ch_{D_2-eNB}, T_{SD_2}, \left\{ \left[DH \left(Ch_{D_1-eNB}', T_{SD_1} \right) \right]_{Pr_{D_1}} \right\}_{PeNB}, \\ Ch_{CH-eNB}, T_{SCH}, \left[DH \left(Ch_{CH-eNB}', T_{SCH} \right), VD_2 \right]_{Pr_{CH}} \end{array} \right)_{PeNB} \quad \text{Equation 3.10}$$

3.3.10.1 Potential Security Threats

The Authentication Request Message, Equation 3.10 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.10.2 Encryption Mechanism

To counter above mentioned attacks, the request message is prepared by using two credentials i.e. challenge and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of D₁. The message also contains request message for eNB with credentials challenge for eNB from CH and timestamp. The message also contains double hash value of challenge solution, timestamp and D₁ validation request from CH to eNB (VD₁) which is signed by the private key of CH. Similarly, the message second portion contains double hash value of challenge solution, timestamp and D₂ validation request from CH to eNB (VD₂) which is signed by the private key of CH. Later the Auth-Req message is signed by the public key of eNB.

As discussed in Table 3.2, usage of challenge and timestamp can mitigate malware attack, timestamps exploitation attack, replay attack, man in the middle attack and modification of data attack. While double hashing the solution of challenge and timestamp

can mitigate weak collision attack, man in the middle attack and pre-image attack and ensure integrity of the data which means no data is modified during the entire communication. The message also used solution of challenge during double hashing process, the purpose of sending challenge is to ensure receiver is a genuine cellular device which means it's not bot hence it also mitigates the denial of service attack. The double hash value is encrypted by private key of the sender CH to ensure the message is sent by the legitimate device thus mitigating the impersonation attack. Device D_1 validation request VD_1 and device D_2 validation request VD_2 is sent to eNB to validate both devices D_1 and D_2 to communicate. This also mitigates rogue device attack. The entire message is encrypted by public key of the receiver to maintain the secrecy of the message.

3.3.10.3 Decryption Mechanism

Once eNB receives the authentication request message from CH, it will use its own private key to decrypt the entire message. When the message is decrypted, it will check challenge given and timestamp. eNB will address the challenge and check either the timestamp is fresh or not. Later, eNB will check double hash values of challenge solution from CH and timestamp. Then CH will match both values, if double hash values i.e generated by eNB and other sent by CH match, it means data integrity is maintained.

3.3.11 Authentication Response Message

Equation 3.11 is an Authentication Response Message where eNB validates both devices D_1 and D_2 and sends CH to forwards validation response to both devices. The security threat associated with this message and how message is encrypted and decrypted is explained as below.

$$\left\{ \begin{array}{l} Ch_{eNB-CH}, T_{SeNB}, [DH(Ch_{eNB-CH}', T_{SeNB})]_{Pr_{eNB}}, \\ \left\{ Ch_{eNB-D_1}, T_{SeNB-D_1}, VD_1' [DH(Ch_{eNB-D_1}', T_{SeNB-D_1}, VD_1')] \right\}_{Pr_{eNB}} \right\}_{P_{D_1}}, \\ \left\{ Ch_{eNB-D_2}, T_{SeNB-D_2}, VD_2' [DH(Ch_{eNB-D_2}', T_{SeNB-D_2}, VD_2')] \right\}_{Pr_{eNB}} \right\}_{P_{D_2}} \right\}_{P_{CH}} \quad \text{Equation 3.11}$$

3.3.11.1 Potential Security Threats

The Authentication Response Message, Equation 3.11 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.11.2 Encryption Mechanism

To counter above mentioned attacks, the request message is prepared by using two credentials i.e. challenge and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of eNB. The message second portion contains response message for D₁ and D₂ with credentials challenge, timestamp and devices D₁&D₂ validation solution VD₁', VD₂' from eNB. The message also contains double hash value of challenge solution, timestamp and validation solution VD₁', VD₂' which is signed by the private key of eNB and encrypted by public key of D₁ and D₂. Later, the Auth-Response message is encrypted by the public key of CH.

As discussed in Table 3.2, usage of challenge and timestamp can mitigate timestamp exploitation attack, replay attack, pre-image attack, man in the middle attack and modification of data attack. While double hashing the solution of challenge and timestamp can mitigate weak collision attack, man in the middle attack and pre-image attack. It also

ensures integrity of data which means no modification during the entire communication. The message also uses solution of challenge during double hashing process. The purpose of sending challenge is to ensure receiver is a genuine cellular device which means it's not bot so it mitigates denial of service attack. The double hash value is encrypted by private key of the sender (eNB) to ensure the message is sent by the legitimate device thus mitigating the impersonation attack. Device validation solution VD_1' and VD_2' are sent to mitigate rogue device attack. The entire message is encrypted by the public key of the receiver to maintain secrecy of the message.

3.3.11.3 Decryption Mechanism

Once CH receives the authentication response message from eNB, it will use its own private key to decrypt the entire message. Once the message is decrypted, it will check challenge given and timestamp. CH will address the challenge and check either the timestamp is fresh or not. Later, CH will check double hash values of challenge solution from eNB and timestamp. Then CH matches both values, if double hash values i.e. generated by CH and other sent by eNB match, it means data integrity is maintained.

3.3.12 Authentication Response Message

Equation 3.12 is an Authentication Response Message where eNB validates device D_1 and CH forwards it to devices D_1 .

$$\left\{ \begin{array}{l} Ch_{CH-D_1}, T_{SCH}, [DH(Ch_{CH-D_1}', T_{SCH})]_{Pr_{CH}}, \\ Ch_{eNB-D_1}, T_{SeNB-D_1} \\ , VD_1' [DH(Ch_{eNB-D_1}', T_{SeNB-D_1}, VD_1')]_{Pr_{eNB}} \end{array} \right\}_{P_{D_1}} \quad \text{Equation 3.12}$$

3.3.12.1 Potential Security Threats

The Authentication Response Message, Equation 3.12 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.12.2 Encryption Mechanism

To counter above mentioned attacks, the request message Equation 3.12 is prepared by utilizing two credentials i.e. challenge and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of CH. The message second portion contains validation response message VD_1' for D_1 signed by private key of eNB. This message contains challenge, timestamp and solution of device validation VD_1' . Later the Auth-Response (CH- D_1) is signed and encrypted by public key of device D_1 .

As discussed in Table 3.2, usage of challenge and timestamp can mitigate timestamp exploitation attack, replay attack, pre-image attack, man in the middle attack and modification of data attack. While double hashing the solution of challenge and timestamp can mitigate weak collision attack, man in the middle attack and pre-image attack. It also ensures integrity of data which means no data is modified during the entire communication. The message also uses solution of challenge during double hashing process. The purpose of sending challenge is to ensure receiver is a genuine cellular device which means it's not bot so it mitigates denial of service attack. The double hashed value is encrypted by private key of the sender (eNB) to ensure the message is sent by the legitimate device thus mitigating the impersonation attack. Device validation solution VD_1' is sent to mitigate rogue device

attack. The entire message is encrypted by the public key of the receiver to maintain secrecy of the message.

3.3.12.3 Decryption Mechanism

Once the D_1 receives the authentication request message from CH, it will use its own private key to decrypt the entire message. Once the message is decrypted, it will check challenge given and timestamp. D_1 will address the challenge and check either the timestamp is fresh or not. Later, D_1 will check double hash values of challenge solution from CH and timestamp. Then D_1 will match both values, if double hash values i.e generated by D_1 and other sent by CH match, it means the data integrity is maintained.

3.3.13 Authentication Response Message (CH-D2)

Equation 3.13 is an Authentication Response Message (CH-D2) where eNB validates device D2 and CH forwards it to device D2.

$$\left\{ \begin{array}{l} \text{Ch}_{\text{CH-D}_2}, T_{\text{SCH}}, \left[\text{DH} \left(\text{Ch}_{\text{CH-D}_2}', T_{\text{SCH}} \right) \right]_{\text{Pr}_{\text{CH}}}, \\ \text{Ch}_{\text{eNB-D}_2}, T_{\text{SeNB-D}_2} \\ \text{VD}_2' \left[\text{DH} \left(\text{Ch}_{\text{eNB-D}_2}', T_{\text{SeNB-D}_2}, \text{VD}_2' \right) \right]_{\text{Pr}_{\text{eNB}}} \end{array} \right\}_{\text{P}_{\text{D}_2}} \quad \text{Equation 3.13}$$

3.3.13.1 Potential Security Threats

The Authentication Response Message (CH-D2) message Equation 3.13 is vulnerable to attacks such as rouge devices attack where a fake device can claim to be CH. Man-in-the-middle attack can be performed by CH where CH can sniff what is going on. All other major form of attacks as well as how they can be executed is discussed in detail in Chapter 2.

3.3.13.2 Encryption Mechanism

To counter above mentioned attacks, the request message Equation 3.13 is prepared by using two credentials i.e. challenge and timestamp. This message also contains double hash value of challenge solution and timestamp which is signed by the private key of CH. The message second portion contains validation response message VD_2' for D_2 signed by private key of eNB. This message contains challenge, timestamp and solution of device validation VD_2' . Later the Auth-Response (CH- D_2) is signed and encrypted by public key of device D_2 .

As discussed in Table 3.2, usage of challenge and timestamp can mitigate timestamp exploitation attack, replay attack, pre-image attack, man in the middle attack and modification of data attack. While double hashing the solution of challenge and timestamp can mitigate weak collision attack, man in the middle attack and pre-image attack. It also ensures integrity of data which means data is not modified during the entire communication. The message also utilizes solution of challenge during double hashing process, the purpose of sending challenge is to ensure receiver is a genuine cellular device means it's not bot thus it mitigates denial of service attack. The double hash value is encrypted by private key of the sender (eNB) to ensure the message is sent by the legitimate device hence mitigating the impersonation attack. Device validation solution VD_2' is sent to mitigate rogue device attack. The entire message is encrypted by the public key of the receiver to maintain secrecy of the message.

3.3.13.3 Decryption Mechanism

Once D_2 receives the authentication request message from CH, it will use its own private key to decrypt the entire message. When the message is decrypted, it will check

challenge given and timestamp. D_2 will address the challenge and check either the timestamp is fresh or not. Later, D_2 will check double hash values of challenge solution from CH and timestamp. Then D_2 will match both values, if double hash values i.e generated by D_2 and other sent by CH match, it means data integrity is maintained.

3.4 Network Model

Figure 3.2 shows a basic network model where LEMAP will be executed and evaluated. There are three important components of our network model (a) eNB and CH (b) Trusted Devices D_1 , D_2 and (c) Trudy. eNB has a specific coverage area in which several mobile devices exist. Devices in near proximity range can communicate with each other directly without communicating through BS as in traditional cellular network. There can be a malicious device “Trudy” in the communication range which can jeopardize communication between two devices. ECC algorithm is used for creation of a secret key for communication where Elgamal is used for sharing secret key information. For challenge scheme, this research introduces a basic challenge-response scheme with a timestamp. eNB is a fully trusted representative of the base station and can handle request from devices and update BS about device information. CH is a forward relay device which receives requests from devices in its area and forwards requests to eNB for authentication and authorization. eNB is able to transfer basic information of the ECC algorithm used for creation of keys. The eNB also forwards the NTL to all devices periodically to decrease the request for initial information. eNB updates the BS with information shared by devices such as trust value, block list and authorizes D2D communication and maintain the trust level between all devices. Elgamal is used for sharing key information.

The mobile devices shown in Figure 3.2 are small mobile phones that have D2D communication capabilities. These devices can calculate secret keys, hashing and perform verification without addition of any new hardware or software capabilities. They can also run a proximity range algorithm to locate neighboring devices. These devices also communicate with Cluster Head (CH) which works as non-transparent relay as they can receive the traffic from all neighboring devices and forward it to eNB. These devices have capability to block any traffic intended to them and can forward the message to CH. These devices are intelligent enough to create and solve challenges as well as create timestamp. Devices are also capable of creating and verifying hash based on SHA v3 algorithm. Trudy is malicious device which has super computation and memory capabilities which acts like a normal trusted device. Trudy is looking for any possible security attack such as DoS, eavesdropping or MITM. Thus, Trudy can be called as super malicious device. It has also established a base trust with eNB to participate in communication. Trudy can manage the entire security algorithm such as timestamp, basic challenge-response scheme, ECC and Elgamal.

The scenario in Figure 3.2 explains multi hop D2D communication where all devices are connected to eNB through CH that works as relay agent. Here Trudy shown in yellow can attack by pretending to be legitimate device. In figure 3.2 (a) there is a device D_1 that is reachable by eNB but can communicate to D_2 through CH which allows multi-hop communication. The scenario shows that there are other devices in the coverage area of other eNBs would like to do D2D communication with devices which are under eNBs coverage. The figure 3.2(b) shows the mode of multi-hop communication where all devices are under the control of eNB but they prefer to communicate directly. There is one Trudy device that